“CAROL I” NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE
(Publishing house with recognized prestige validated by the National Council
for Attestation of University Degrees, Diplomas and Certificates)

“Carol I” National Defence University
Panduri Street no. 68-72, 5th District, 050622 Bucharest
Phone: +40 21 319 48 80 Fax: +40 21 319 48 66

ISSN 2668-201X
ISSN-L 2668-201X

5 948490 380354 24003

PROCEEDINGS 2024

”CAROL I” NATIONAL DEFENCE UNIVERSITY
COMMAND AND STAFF FACULTY

PROCEEDINGS

THE 20TH INTERNATIONAL SCIENTIFIC CONFERENCE

STRATEGIES XXI

”TECHNOLOGIES, MILITARY APPLICATIONS, SIMULATION AND RESOURCES”

MARCH 28, 2024
BUCHAREST, ROMANIA

ROMANIA
MINISTRY OF NATIONAL DEFENCE
„Carol I" National Defence University
The Command and Staff Faculty

PROCEEDINGS

THE 20TH INTERNATIONAL SCIENTIFIC CONFERENCE

"*STRATEGIES XXI*"

”TECHNOLOGIES – MILITARY APPLICATIONS, SIMULATION AND RESOURCES"

SCIENTIFIC EDITORS:
Eugen MAVRIȘ, PhD
Valentin DRAGOMIRESCU, PhD
Ștefan-Antonio DAN-ȘUTEU, PhD
Ioana ENACHE, PhD
Cosmin OLARIU, PhD
Ion ROCEANU, PhD
Niculai-Tudorel LEHACI, PhD
Daniel ROMAN, PhD
Adi MUSTAȚĂ, PhD

MARCH 28, 2024
BUCHAREST, ROMANIA

INTERNATIONAL SCIENTIFIC COMMITTEE:

- Col. Prof. Alexandru HERCIU, PhD, NDU Command and Staff College
- Col. Assoc. Prof. Dan COLESNIUC, PhD, NDU
- Col. Assoc. Prof. Daniel ROMAN, PhD, NDU Command and Staff Faculty Vice-Dean for Research
- Col. Assoc. Prof. Pătru PÎRJOL, PhD, NDU Command and Staff College
- Col. Prof. Marilena-Miorica MOROŞAN, PhD, NDU Command and Staff College
- Col. Prof. Ion ANDREI, PhD, NDU Command and Staff College
- Col. Assoc. Prof. Alin-Dumitru PELMUŞ, NDU Command and Staff College
- Col. Assoc. Prof. Cătălin CHIRIAC, PhD, NDU Command and Staff College
- Lt.col. Prof. Adi MUSTAŢĂ, PhD, Interdisciplinary Doctoral School Director
- Lt.col. Assoc. Prof. Răzvan ENACHE, PhD, NDU Command and Staff College
- Lt.col. Assoc. Prof. Petrişor PĂTRAŞCU, PhD, NDU Command and Staff College
- Assoc. Prof. Dănuţa-Mădălina SCIPANOV, PhD, NDU Command and Staff College
- Assoc. Prof. dr. Diana-Elena ŢUŢUIANU, PhD, NDU Command and Staff College
- Assoc. Prof. Ana-Maria CHISEGA-NEGRILĂ, PhD, NDU Command and Staff College
- Assoc. Prof. Adriana RÎŞNOVEANU, PhD, NDU Security and Defence Faculty
- Assoc. Prof. Alba Iulia Catrinel POPESCU, PhD, NDU National Defence College
- Col. Assoc. Prof. Alexandru STOICA, PhD, NDU National Defence College
- Crăişor-Constantin IONIŢĂ, PhD, NDU Centre for Strategic Defence and Security Studies
- Adrian Victor VEVERA, PhD, Eng., National Institute for Research & Development in Informatics, Bucharest, Romania
- Carmen Elena CÎRNU, PhD, National Institute for Research & Development in Informatics, Bucharest, Romania
- Alexandru GEORGESCU, PhD, National Institute for Research & Development in Informatics, Bucharest, Romania
- Ella CIUPERCĂ, PhD, National Institute for Research & Development in Informatics, Bucharest, Romania
- Jeana CÎMPINEANU, PhD, Euro-Atlantic Resilience Centre, Bucharest, Romania
- Dănuţ MAFTEI, PhD, Romanian National Cyber Security Directorate
- Assoc. prof. Ioan VIRCA, PhD, eng., Vice-Rector for Scientific Research Land Forces Academy, Sibiu, Romania
- Assoc. prof. Lucian ISPAS, PhD, eng., Vice-Rector for Academics Land Forces Academy, Sibiu, Romania
- Col. Prof. Cezar VASILESCU, PhD. eng., Director Postgraduate School of Studies DRESMARA, Braşov
- Assoc. Prof. Maria CONSTANTINESCU, PhD., DRESMARA, Braşov
- Col. Prof. Adrian LESENCIUC, PhD, Air Security Systems Faculty Dean, ”Henri Coandă” Air Forces Academy, Braşov, Romania
- Col. Assoc. Prof. Laurean GHERMAN, PhD, Air Security Systems Faculty Vice-Dean for Education, ”Henri Coandă” Air Forces Academy, Braşov, Romania
- Col. Assoc.Prof. Cătălin CIOACA, PhD, Aeronautic Management Faculty Vice-Dean for Education, ”Henri Coandă” Air Forces Academy, Braşov, Romania
- Cdor. Assoc. Prof. Paul BURLACU, PhD eng., ”Mircea cel Bătrân” Naval Academy, Constanţa, Romania
- Cdor Assoc. Prof. Dinu ATODIRESEI, PhD eng., ”Mircea cel Bătrân” Naval Academy, Constanţa, Romania
- Lt. cdor. Assoc. Prof. Ovidiu CRISTEA, PhD eng., ”Mircea cel Bătrân” Naval Academy, Constanţa, Romania
- Prof. Ion CHIORCEA, PhD eng., „Mircea cel Bătrân” Naval Academy, Constanţa, Romania
- Prof. Florin NISTOR, PhD, „Mircea cel Bătrân” Naval Academy, Constanţa, Romania
- General (ret.) Prof. Teodor FRUNZETI, PhD, Titu Maiorescu University, Bucharest, Romania
- Col. Alexandru KIŞ, PhD, NATO HUMINT Centre of Excellence
- Assoc. Prof. Ivona RAPAN, PhD, Romanian Academy
- Lucian DUMITRESCU, PhD, Romanian Academy
- Georgica PANFIL, PhD, European Security and Defence College, Belgium
- Col. Assoc. Prof. Bogdan-Cezar CHIOSEAUA, PhD, Head of Management and Military Science Department from “Henri Coandă” Air Force Academy, Braşov Romania
- Col. Assoc. Prof. Constantin GRIGORAŞ, PhD, Land Forces Academy, Sibiu, Romania
- Col. Assoc. Prof. Laviniu BOJOR, PhD, Land Forces Academy, Sibiu, Romania
- Lt. col. Prof. Tudorache PAUL, PhD, Land Forces Academy, Sibiu, Romania

ORGANIZING COMMITTEE:

Chairman:

- Maj.gen. Eugen MAVRIŞ, PhD, Commandant (Rector), “Carol I” National Defence University, Romania

- Col. Prof. Valentin DRAGOMIRESCU, Ph.D. Prof., Vice-Rector for Education “Carol I” National Defence University, Romania
- Col. Assoc. Prof. Ştefan-Antonio DAN-ŞUTEU, PhD, NDU Vice-Rector for scientific research and inter-institutional relations
- Col. Prof. Ioana ENACHE, PhD, NDU Vice-Rector for Continuing Education, Relationship with Students and Career Guidance
- Col. Assoc. Prof. Cosmin Florian OLARIU, PhD, Vice-Rector for International Relations
- Col. (r) Prof. Ion Roceanu, PhD, Director of the Council for Doctoral Studies
- Col. Prof. Niculai-Tudorel LEHACI, PhD, NDU Command and Staff Faculty, Vice-Dean for Education
- Col. Assoc. Prof. Daniel ROMAN, PhD, Command and Staff Faculty Vice-Dean for Scientific Research
- Lt.col. Prof. Adi MUSTAŢĂ, PhD, Interdisciplinary Doctoral School Head
- Assoc. Prof. Ivona RAPAN, PhD, Romanian Academy

Members:

- Col. Gheorghe LUCA, PhD, NDU Command and Staff Faculty
- Maj. senior instructor, Gabriela NICOARĂ, PhD, NDU Command and Staff College
- Navy Capt. senior instructor, Ionuţ CIORANU, PhD Candidate, NDU Command and Staff Faculty
- Navy Capt. senior instructor, Alexandru Lucian CUCINSCHI, PhD Candidate, NDU Command and Staff Faculty
- Navy Capt. senior instructor, Valentin TOTIR, PhD Candidate, NDU Command and Staff Faculty
- Lt. col. senior instructor, Ionuţ-Cosmin BUŢĂ, PhD Candidate, NDU Command and Staff Faculty
- Lt. col. senior instructor, Daniela-Elena HRAB, PhD Candidate, NDU Command and Staff Faculty
- Lt. col. senior instructor, Adrian MIREA, PhD Candidate, NDU Command and Staff Faculty
- Lt. col. senior instructor, George-Ion TOROI, PhD Candidate, NDU Command and Staff Faculty
- Lt. col. senior instructor, Claudiu Valer NISTORESCU, PhD Candidate, NDU Command and Staff Faculty
- Capt. cdor. senior instructor, Claudiu-Cosmin RADU, PhD Candidate, NDU Command and Staff Faculty
- Capt. cdor. senior instructor, Cătălin BALMUŞ, PhD Candidate, NDU Command and Staff Faculty
- Maj. superior instructor, Ana-Maria MERLUŞCĂ, PhD Candidate, NDU Command and Staff Faculty
- Maj. superior instructor, Petru-Marian VEREŞ, PhD Candidate, NDU Command and Staff Faculty
- Col. Constantin PAGNEJER, PhD, NDU General Administrative Director

Romanian National Cyber Security Directorate:

- Maria-Manuela CATRINA, PhD Candidate
- Dănuţ MAFTEI, PhD
- Florin NECULA

Euro-Atlantic Resilience Centre:

- Adrian DUŢĂ, PhD
- Jeana CÎMPINEANU, PhD
- Daniela MUNTEANU, Phd candidate
- Camelia BOTEZATU

National Institute for Research & Development in Informatics:

- Adrian Victor VEVERA, PhD, Eng.
- Alexandru GEORGESCU, PhD
- Carmen Elena CÎRNU, PhD
- Ella CIUPERCĂ, PhD

Administrative and IT&C support:

- Col. Doru ENACHE
- Col. Florin BÎRSĂ
- Col. Sorin RUSA
- Col. Adrian COVACI
- Lt.col. Mariana TUDOR
- Lt.col. Florin GÂNDILĂ
- Octavian CHIRIAC
- Laura MÎNDRICAN
- Valentina ILINCA
- Andreea GÎRTONEA
- Carmen IRIMIA
- Andreea BREBU

- Capt. Tiberiu ION
- Iustin ŞTEFĂNESCU
- Cătălin RADU
- Draga CRĂCIUN
- Alina POP
- Ana-Maria CĂLINA
- Florin DUMITRA
- Gabriela MOȚ
- Nicolae SÎRBU
- Florina GRUIA
- Iuliana MIHAI
- Otilia LEHACI
- Ana Raluca STAN
- Ana-Maria DUMITRU
- Eugen SATNOIANU
- Ioana MATEESCU

CONFERENCE AGENDA
POLICY PANEL: ”Emerging threats are shaping the future of defense”

- **Moderator:** Col. Assoc. Prof. Ștefan-Antonio DAN-ȘUTEU, PhD

Keynote speakers :

- Lt.gen. Dragoș-Dumitru IACOB, PhD – Deputy Chief of Defence Staff
- Maria-Manuela CATRINA, PhD candidate – Vice-president Romanian National Cyber Security Directorate – DNSC
- Adrian DUȚĂ, PhD – Gl.(r) Vice-president Euro-Atlantic Resilience Centre – E-ARC
- Alexandru GEORGESCU, PhD – Critical Infrastructure Expert National Institute for Research & Development in Informatics – ICI
- Dănuț MAFTEI, PhD, Romanian National Cyber Security Directorate –DNSC

Panel moderators:
PANEL 1: CHALLENGES WITHIN THE NEW NATIONAL AND EURO-ATLANTIC RESILIENCE CONTEXT
Moderators:

- Lt.col. Prof. Adi MUSTAŢĂ, PhD, Interdisciplinary Doctoral School Director
- Assoc. Prof. Ivona RAPAN, PhD, Romanian Academy

PANEL 2: TECHNOLOGIES - MILITARY APPLICATIONS, CYBERDEFENCE, MODELLING AND SIMULATION
Moderators:

- Gl.bg. Gabriel MUNTEANU, Headquarters Multinational Corps South-East – HQ MNC-SE
- Col. Assoc. Prof. Petar MARINOV, PhD, Rakovski National Defense College, Bulgaria
- Col. Assoc. Prof. Daniel ROMAN, PhD, NDU Command and Staff Faculty

PANEL 3: MULTI-DOMAIN OPERATIONS, RESOURCES MANAGEMENT AND LOGISTICS
Moderators:

- Col. Prof. Niculai-Tudorel LEHACI, PhD, NDU Command and Staff Faculty, Vice-Dean for Education
- Col. Prof. Marilena-Miorica MOROŞAN, PhD, NDU Command and Staff College
- Navy Capt. senior instructor, Valentin TOTIR, PhD Candidate, NDU Command and Staff Faculty

PANEL 4: HYBRID WARFARE AND CRITICAL INFRASTRUCTURES PROTECTION
Moderators:

- Lt.col. Assoc. Prof. Petrisor PĂTRAȘCU, PhD
- Dănuţ MAFTEI, PhD, Romanian National Cyber Security Directorate
- Lt. col. senior instructor, Ionuţ-Cosmin BUŢĂ, PhD Candidate, NDU Command and Staff Faculty

Desktop publishing: Valentina ILINCA
Cover designer: Andreea GÎRTONEA
ISSN (online) 3045-1396; ISSN-L 2668-201X

SPONSORS:

AUTONOMUS FLIGHT TECHNOLOGIES R&D SRL

www.aft.ro

INTERACTIVE SOFTWARE SRL

www.intersystems.ro

PROCEEDINGS

THE 20TH INTERNATIONAL SCIENTIFIC CONFERENCE
“*STRATEGIES XXI*”

”TECHNOLOGIES – MILITARY APPLICATIONS, SIMULATION AND RESOURCES”

GRUP PHOTO

TABLE OF CONTENTS

SECTION 1

CHALLENGES WITHIN THE NEW NATIONAL AND EURO-ATLANTIC RESEILIENCE CONTEXT

1053477-3045-1396-24-01

TRANSFORMING TRANSATLANTIC SECURITY: WITH ADJECTIVES

Hristina DOBREVA, PhD.
Senior Assistant, PhD in National and International Security,
Rakovski National Defence College, Sofia, Bulgaria
E-mail: h.dobreva@rndc.bg

Abstract*: Traditionally collective security coexists with collective defence. Although security and defence are complementary in the transatlantic system, their differentiation clarifies the concepts. The paper applies security concepts to EU security to find elements of common, comprehensive security within the EU. NATO remains a common security provider. Thus, EU widens and NATO deepens the security concept. NATO-EU security however is still a matter of ad-hoc decisions, unfixed combination of adjectives.*
Keywords: *security concept, defence, transatlantic, NATO-EU relations.*

Introduction

Security is a flexible concept in NATO-EU relations. 1975 Helsinki process accepts a wide definition of security to reflect complex interdependence. While the defence concept is a stable characteristic of the functioning of the system, the security concept is flexible and some of its versions (human, or comprehensive) broaden its contents, other versions (national-now homeland) remain constant, and still others (common) deepen its contents. Thus, adjectives such as “human”, “comprehensive” and “homeland” enter the transatlantic security debate at different stages. However, these “securities with adjectives” are not universally applicable-thus unreliable explanatory bases for the future NATO-EU relations.

I. Deepening and Widening of the Security Concept

Adding different adjectives to security concept makes it liable to different theoretical interpretations. The conventional definition of security stems from Realism in the form of national security. Nation and state coincide. It appears in the Westphalian order of states (Moller, 2000). Cooperative, comprehensive and human security appear as the main challengers (Bajpai, 2000).

In 1982 the Palme Commission delivers a report to the UN, where it introduces the concept cooperative (mutual or common) security. The idea opposes disarmament and mutual restraint to anarchy, solving Cold War security dilemma through joint actions. Thus, cooperative security deepens the security concept in the military area. On the other hand, both comprehensive and human security widen the concept as they include dimensions beyond the military one.

Initially, human security, as a post-Cold War-1994 UNDP creation, originates as an explanation of insecurities in the third world. Security becomes a synonym of development. Concept operationalization lacks precision and is found in three versions: military (less casualties), economic (sustainable development), and legal (defending human rights) (Acharya, 2002). The increase of the number of internal conflicts in the developing countries at the beginning of the ’90s leads to alternative security outlooks. International terrorism is among the threats to human security. National sovereignty and security of the people are treated with equal importance (Jolly, Ray, 2006 - www.hdr.undp.org). Military force is a last resort for the provision of human security (Axworthy, 1999: 359). Building human security is a process that should involve diverse actors, short-term humanitarian actions and long-term strategies for peace and sustainable development (Axworthy, 1999: 360).

Comprehensive security as a most recent concept has tried to explain the unity of different security dimensions-military, economic, political, environmental, cultural (Moller, 2000). However, the threat of excessive securitization of all spheres remains.

After 11/09/2001 security has been transformed from human to homeland. Homeland security resembles the classical national security. Homeland security is an American prototype. Presidential order of 08.10.2001 creates a Homeland Security Office. It aims at achieving coordination in implementing American Security Strategy against terrorism. This strategy is a comprehensive long-term national plan supported by the federal budget for enhancing key areas as counter-reaction in case of bio-terrorism, border and airport security.

Table no. 1: Different types of security

Types of security	Threats to security	Object of security	Widening/deepening
national	Threats to national sovereignty and territory	State	Classical concept
homeland	Same as above	State	Tight concept after 11/09/2001
collective	Military threats	State and institutions above the state	Deepening
cooperative	Security dilemma	State	Deepening
human	Threats to human survival, dignity and development	Individual and state	Widening
comprehensive	Different dimensions	Different	Widening

Applying Security Concepts to EU and NATO Security

2.1. EU Security

On the one hand, the prevention of any future threat of war is the stimulus for collective European action at the very beginning of European integration. This approach to European security builds on common security. According to the above-mentioned security definitions, ECSC (European Coal and Steel Community), which is the basis of the contemporary EU, focuses on the economic dimension of security, an "approach of common security to the economic security" (Moller, 2000). The idea for a network of mutual dependence becomes an element of classical liberalism and neo-functionalism. Multilateralism starts with a bilateral agreement (in this case between France and Germany). Mutual dependencies, multilateralism, and the spillover effect broaden the integration idea and gradually include more and more areas of mutual dependence, providing a comprehensive security foundation. Thus, common security transforms into a comprehensive security.

On the other hand, the opposite assumption is to be found. Common security is based on human security or economic development. The evidence in support of that argument is that the Schuman declaration and plan integrate security and economic development, an idea of human security concept as well. Economic development becomes possible after giving away sovereignty in vital areas of military industry at that time (coal and steel). Economic development needs solidarity, economic unification, accountability to UN bodies (The Schuman Declaration of 9 May 1950). It plans the creation of a European federation. The Schuman Plan is based on four community principles, which build an institutional approach:

1) Supreme role of the institutions; 2) institutional independence and accountability; 3) institutional cooperation and a specific function to each institution; 4) equality between member states. J.Mannet's speech on Schuman's plan (J. Mannet, in Fontaine 2000: 17) argues that a fusion of peoples' interests should be achieved, not just an effort to maintain a balance of these interests. In this way, "a union between people" rather than a coalition between states has been formed.

An important moment in building EU security is the 1992 Maastricht treaty (Treaty of the European Union) creating Common Foreign and Security Policy (CFSP) as a second pillar of the EU (http://europa.eu/scudplus/bg/). CFSP creates a political union with common foreign and defence policy. European political community, formally institutionalized with the Single European Act of 1987, is based on consultations between member-states. CFSP needs intergovernmental cooperation and consensus in decision-making and has instruments as common strategies, positions and joint actions. The EU Constitution of 29/10/2004 introduces a minister of external affairs and external affairs services. The instruments are limited to decisions and international agreements. European security resembles a combination of national and collective security (enhanced national element). Its reflection is the European Security Strategy (ESS). ESS determines five threats to European security: 1) Terrorism; 2) Dissemination of weapons of mass destruction (biggest threat); 3) Regional conflicts; 4) Bad governance; 5) Organized crimes. Threats are more diverse, less visible and predictable and resemble the above-mentioned human security concept. Coping with these threats requires Europe to be: 1) more active (early intervention, crisis management, crisis prevention); 2) more capable; 3) more coherent (joining resources and capabilities of EU and non-EU countries) (http://ec.europa.eu/world/peace). "Effective multilateralism" has been mentioned as a strategy for action in ESS. Effective multilateralism or legitimacy of action (Kaldor, Martin, Selchow 2007: 278) is considered a dimension of human security.

According to some authors EU is already practicing human security, although named as crisis management, civil-military coordination, and conflict prevention (Kaldor, Martin, Selchow 2007:273).

2.2. NATO Security

After the end of the Cold War NATO undergoes a transformation in cooperative security, NATO expands its tasks to include: 1) Cooperation with recent Cold War enemies; 2) Conflict management in previous out-of-NATO-area regions (Haglund 2004: 20). The first task opens the Alliance, the second-military involves NATO military on the Balkans. 1999 NATO strategic concept (www.nato.int/docu/pr.1999) supports primarily security enhancement, prosperity and democracy in the Euro-Atlantic region - i.e. a democratic peace idea. The 1999 Strategic Concept starts the development of Euro-Atlantic security structure, where NATO plays a central role. The broad approach to security adds political, economic and social factors to security issues in order to respond to new risks as ethnic conflicts, economic decay, terrorism, dissemination of weapons of mass destruction. Articles 5, 6 (defence against threat of aggression or an attack against any NATO member) and article 7 (conflict prevention and crisis management) of the Washington Treaty serve as the foundation. Internal reform includes a new command structure - Combined Joint Task Force, building of European Security and Defence Identity (ESDI) within NATO. The deterrent role of American, British and French nuclear forces provides a supreme security guarantee.

2006 Riga Summit Declaration (www.nato.int) emphasizes solidarity and inseparability of ally security. NATO is considered a "main forum of security consultations" between North America and European allies. According to NATO General Secretary Jaap de Hoop Scheffer (29.01.2007), there is no security without development and no development without security. Challenges need to be addressed by a comprehensive approach to security, coordinating military and civil means (www.nato.int/docu/update/2007/01), (www.europarl.europa.eu -

NATO and the EU   Time for a new Chapter). A global approach to security could correspond to global threats like terrorism, weapons of mass destruction, bad governance. The need for a comprehensive security has been demonstrated by Afghanistan's reconstruction, development, and democracy-building. The 2006 Riga Summit (www.nato.int/docu/review/ - The Comprehensive Political Guidance: A primer) uses a wide approach to security in terms of NATO instruments for crisis management, cooperation with non-NATO member states.

2.3. NATO-EU strategic partnership - what kind of security?

In essence NATO-EU strategic partnership is based on flexible coalitions and a strategic dialogue. On the one hand, EU uses this partnership to develop ESDP but EU uses the term for its relations with the US, Japan, China, Canada, India and possibly Russia as well (www.ec.europa.eu/world/peace). On the other hand, US position is different because it emphasizes the threat of overlapping between NATO and EU in the area of transatlantic security. It accounts for EU's incapability of organizing alone a massive military operation for European defence (www.acus.org, F.Burwell 2006:4). The new "security architecture" (Burwell, Gompart, Lebl and others 2006: 27) stems from a coordination mechanism between the NATO Reaction Force (NRF) and EU Battle Groups (EUBG) (www.nato.int, europa.eu.int). NRF serves as a catalyst for the transformation of the NATO and EU armed forces.

The Strategic partnership was initiated in 2002 (www.consilium.europa.eu-EU-NATO declaration on ESDP). The common aim of collective security and stability leads to three decisions: 1) EU provides participation of non-EU European NATO members within ESDP, 2) common capabilities – NATO supports ESDP and gives EU access to NATO military planning capabilities, 3) both EU and NATO build capabilities in open relations with each other. Javier Solana considers strategic partnership a response to similar need of peace and stability, a response to new threats as organized crime, migration, diseases, terrorism, weapons of mass destruction (www.ue.eu.int-Article by Javier Solana…). These threats are in the spirit of human security concept. Solana suggests a blurring between internal and external security boundaries, between political and military issues, between crisis prevention and crisis management. Unlike the American concept of "homeland security", which starts inside the people, he uses the concept "homeland defence", which starts outside. According to him, EU's early participation in conflict prevention is an illustration of "smart security" - i.e. capability to work with partners.

Despite the efforts from both sides, a common mechanism for decision-making is still lacking and the approach is case-by-case. Comprehensive security concept differs in meaning from NATO's "comprehensive approach to security" (2007 Jaap de Hoop Scheffer), which simply broadens the means for achieving a common security. Riga's definition for NATO as a forum supports the argument that NATO and EU have built a non-formal regime, based on consensus and ad-hoc agreements. It could be regarded as a common-antipathy-regime (common threats as terrorism and weapons of mass destruction), a coordination rather than cooperation.

Conclusions

NATO and EU security policies, as well as NATO-EU "strategic partnership" have been explained with the help of the security concept. The paper applies the analysis to primary sources as official documents. EU widens the security concept and ESS's "effective multilateralism" is a characteristic of human security. NATO deepens the security concept. There is agreement on the nature of threats and the need for multinational operation. However, "strategic partnership" is still a forum for discussion, informal regime for ad-hoc coordination, rather than an established decision-making mechanism.

Some further fields of analysis include: 1) theoretical linkage of security and defence concepts, 2) the nature of the project ESDI within NATO, which includes both clarifying ESDI (European Security and Defence Identity) and NATO identity. For example, on the one hand, EU's role could be clarified with the help of the human security concept. Thus, EU could improve NATO-UN relations (or US-UN relations). On the other hand, NATO could be transformed into a new two-pillar partnership between the US and the EU.

BIBLIOGRAPHY:

1. Acharya, A. 2002. "Security and security studies after September 11: some preliminary reflections", *Institute of Defence and Strategic Studies*, Singapore, N23:16-32 (www.ciao.org)
2. Axworthy, L. 2005. "Human Security: Safety for People in a Changing World": 355-360 in *Crosscurrents-International Relations*, 4th edition, ed. by Mark Charlton, Thompson-Nelson Ltd.
3. Burwell, F. 2006. "Project on the future of NATO-EU", Transatlantic Relations Programme, Issue Brief, www.acus.org, (www.ciao.org)
4. Burwell, F. and others .2006. "Transatlantic Transformation: Building a NATO-EU Security Architecture", policy paper, Atlantic Council of the United States, (www.ciao.org)
5. Fontaine, P. 2000. "The Schuman Plan: The Birth of Community Europe", p. 17-22; Annexes – "Declaration of May 1950", p. 36-38; "A new idea for Europe – The Schuman declaration"
6. Jolly, R. and D. Ray. 2006. "The Human Security Framework and National Human Development Reports: A Review of Experiences and Current Debates", *United Nations Development Programme*, Human Development Report Office, National Human Development Report Series, NHDR Occasional Paper 5. www.hdr.undp.org
7. Kaldor, M., M. Martin and S. Selchow .2007. "Human Security: a New Strategic Narrative for Europe," *International Affairs* 83:2:273-288.
8. Haglund, D. 2004. "Western Europe and the Challenge of the "Unipolar Moment": Is Multipolarity the Answer?"in *Journal of Military and Strategic Studies*, Vol.6:4 (www.ciao.org)
9. Møller, B. 2000. "The Concept of Security: The Pros and Cons of Expansion and Contraction", *Copenhagen Peace Research Institute*, (www.ciao.org)
10. Schefer, Jaap. 2006. "Global NATO: Overdue or Overstretch", Speech at the SDA Conference, Brussels, 6 November 2006, www.nato.int
11. Schefer, Jaap. 2007. "NATO and the EU: Time for a New Chapter", Keynote speech by NATO Secretary General, 29.01.2007, www.europarl.europa.eu
12. Smith, S. 2002. "The Concept of Security Before and After September 11", *Institute of Defence and Strategic Studies,* Singapore, N23:1-16 (www.ciao.org)
13. Solana, J. 2002. "The European Union and NATO, A Strategic Partnership" in the *European Voice* on 21 November 2002, www.ue.eu.int
14. www.homelandsecurity.gov
15. www.humansecurity.gc.ca
16. www.hdr.undp.org
17. www.un.org
18. www.europa.eu/scadplus/leg
19. www.consilium.europa.eu
20. www.homelandsecurity.gov – The President's Plan to Strengthen our Homeland Security
21. www.nato.int – The Alliance's Strategic Concept, Washington, 23 - 24 April 1999
22. http://ec.europa.eu/world/peace/- "The EU: A global player in security", Javier Solana High Representative for the EU's Common Foreign and Security Policy (CFSP)

23. www.consilium.europa.eu- Remarks by Javier Solana, EU High Representative for the Common Foreign and Security Policy following the agreement on the establishment of EU-NATO permanent arrangements, Brussels, 16 December 2002
24. www.nato.int- The Comprehensive Political Guidance: A primer
25. http://www.nato.int/docu/pr/1999/p99-064e.htm Washington Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Washington, D.C. on 24th April 1999
26. http://www.nato.int/docu/pr/2002/p02-142e.htm,EU-NATO Declaration on ESDP-16.12.2002
27. http://www.nato.int/docu/pr/2006/p06-150e.htm#nato_eu Riga Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Riga on 29 November 2006
28. http://www.nato.int/docu/basictxt/b061129e.htm Comprehensive Political Guidance
29. Endorsed by NATO Heads of State and Government on 29 November 2006
30. http://www.nato.int/issues/nato-eu/practice.htmlNATO-EU: A strategic partnership

1053477-3045-1396-24-02

WHY NEW WEAPONS ARE NOT ALWAYS ENOUGH TO WIN A WAR? LESSONS FROM RUSSIAN-UKRAINIAN WAR

Claudiu-Valer NISTORESCU, PhD. candidate
Lieutenant colonel, Advanced Instructor, PhD Candidate,
„Carol I" National Defence University, Bucharest, Romania
E-mail: nistorescu.claudiu@unap.ro

Abstract*: The Russian aggression against Ukraine has significantly altered the international security environment. Traditional democracies are now faced with new challenges and are seeking innovative solutions to address them. The conflict between Russia and Ukraine involves two powerful armies employing their respective doctrines, warfare knowledge, and advanced weapon systems to gain an advantage. Western countries have been supporting the Ukrainian armed forces by providing them with sophisticated weapons and technologies, which have enhanced their chances of success. The combat effectiveness of these new capabilities is undeniable. However, the failure of the 2023 Ukrainian Summer Offensive to achieve its stated objective necessitates an evaluation of the overall impact of these capabilities. This article aims to identify the limitations of new weapon systems and solutions to improve and exploit their effects on the battlefield in an objective and balanced manner.*

Keywords: *new weapon systems, combat adaptation, battlefield asymmetries, combined arms approach, offensive manoeuvre.*

Introduction

On February 24th, the conflict between the Russian Federation and Ukraine began. Since then, two near-peer armies have fought and contested each other in all military domains. Although both the Russian and Ukrainian armies aimed to defeat their opponent, they experienced both successes and failures in combat during more than two years of fighting. Those years of high-intensity fighting reveal a complex confrontation including a lot of asymmetries: economic disparities, legitimacy, the existence of alliances and international support, the quality of leadership, commanders' professionalism, and the ability to operate in all military domains.

When discussing international support, professional competence, leadership, or morale, it is clear that Ukrainians have an advantage. The Russian forces possess superior capabilities that enable them to strike Ukrainian forces, critical infrastructure, and citizens' homeland throughout the entire country. However, Western support managed to somehow counter the complexity of the Russian strikes, reducing their effectiveness. The Ukrainian military has access to a range of advanced weaponry, including Javelin anti-tank missiles, HIMARS rocket and artillery system, Patriot air defense system, Excalibur munitions, Storm Shadow missiles, Leopard tanks, and Bradley infantry fighting vehicles. These weapons enhanced Ukraine's capacity to resist, and many experts predicted a close victory due to their devastating effects (William Courtney 2023). The end of 2023's Ukrainian counteroffensive indicates that they have not yet achieved victory. However, the Russian forces still lack the strength to succeed.

In this context, we are interested in determining how Western weapons performed on the battlefield. The analysis also aims to identify the factors that might enhance the weapons' effectiveness or diminish their success on the battlefield.

At the centre of the analysis lie three main research questions:

- What are the historical milestones for using new weapons to try to win a war?
- What factors enable the operational success of new weapons systems and what factors limit their potential?
- What are the potential solutions to mitigate the limitations of the new weapons in order to enhance their effectiveness?

To answer these questions objectively, we analysed studies and research reports from respected Western institutes and research centres, as outlined below. Information on operations is provided by credible sources, such as the North Atlantic Alliance and member state institutions. We also considered the opinions of military and security experts in our assessment. As this conflict is ongoing, it is important to note that certain data and information may not be available due to information security reasons or may have been altered as a result of information operations carried out by both parties.

1. Historical considerations

The development of new weapons, technologies, and combat equipment has always shaped warfare. Experts have identified five distinct generations in the development of modern warfare, differentiating them based on the impact generated by the employment of weapon systems and military equipment. The first generation of warfare, characterised by the use of line and column tactics, lasted from the Peace of Westphalia until the second half of the 19th century, but with the development of the machine gun, these tactics became irrelevant and were abandoned. Second-generation modern warfare was developed mainly by the French Army during the First World War and until around 1930. Its main characteristic is the tendency to completely destroy the enemy by concentrating overwhelming firepower. This approach aims to achieve a decisive victory by eliminating the enemy's ability to fight back (William S. Lind 2015, 110). The third generation relied more on speed and less on firepower. Its emergence is a consequence of the development of aviation and armoured, including the self-propelled artillery needed to provide fire support to mechanised combat formations. The German army, in the years leading up to the 2nd World War, theorised the concepts specific to this type of warfare. The tactics employed by the Germans, known as Blitzkrieg, clearly outperformed those of the French army, which was considered to be the most prepared army before the start of the war. Static and positional defences and the massing of overwhelming firepower on the Maginot line by the French were irrelevant against the armoured divisions that penetrated the Ardennes.

Fourth and fifth-generation warfare is a modern phenomenon characterized by low-intensity and geographically limited armed conflicts. These conflicts are often ambiguous, asymmetrical, and irregular, involving the use of unconventional tactics. States that employ these methods also retain the option of using conventional forces. In this context, armed forces must act according to the principles and fundamentals of third-generation warfare as a minimum requirement for success in this type of conflict. Flexibility, agility, and versatility of forces are imperative, as are initiative and both critical and creative thinking by commanders. The dimensions of fourth and fifth-generation warfare are significantly shaped by the operations in informational and cognitive domains.

Contemporary analysis indicates that regardless of the generation of warfare, three main trends have emerged: *increasing the range of weapons, enhancing precision, and improving lethality* (Biddle 2004, 22-28). In this context, it could be assumed that military organizations have always refined their doctrines, tactics, and procedures in a continuous effort to evolve and adapt to the battlefield’s requirements, especially due to technological development. Therefore, conceptual and procedural innovations were driven by scientific breakthroughs that gave armies an opportunity to build new capabilities.

New technologies and weapon systems have often been a versatile tool that allows military commanders to achieve a position of relative advantage over the enemy. By exploiting this advantage, even if it is materialized at the strategic, operational, or tactical level of operations, one side may have the opportunity to win a clash, a battle or even a war. However, success is not guaranteed.

In the 1st World War, military experts and scientists were searching for a solution to break a prolonged stalemate. New weapons had arisen in an attempt to gain a tactical asymmetry in order to break the enemy's battle positions. During the war, military commanders believed that weapons such as airplanes, tanks, and poison gas would give them an advantage on the battlefield. While some gains were made, these weapons ultimately had a limited impact on the overall outcome of the war. The number of soldiers, strength of alliances, and resolute support of the population were ultimately more decisive factors.

In 2nd World War, the German Army by deploying its armored division as a combined arms capability obtained a super weapon that crashed the French Army in a few weeks. The Arden's strategic surprise was augmented by a doctrinal one, catching the French unprepared for this type of war. This approach proved to be more lethal on the Eastern Front, at least in the initial phase of the Barbarossa operation. One year later, the Soviet Army managed to adapt and mirror German's tactics, weapons, and organisation. This allowed them to defeat the Germans at Stalingrad, Kursk, and lately in Berlin. However, in the end, the German Army was ultimately defeated, instead of trying to take advantage of new innovative weapons like V2 missiles. But, the Second World War was the scene of the first use of a powerful weapon that had the power to end the war, at least in one part of the world. The nuclear weapon changed the dimensions of war at that time and has shaped the geopolitical and geostrategic environment ever since.

Military art continued to evolve under the sign of technological innovations. Thirty years later, the Egyptian Army surprised their traditional enemy, the Israeli Defence Force/IDF. The Yom Kippur War is an example of strategic and operational surprise, but also a technological one. The use of new Soviet surface-to-air missiles and anti-tank weapons by the Egyptians negated Israel's superiority in armoured and air capabilities. However, the IDF managed to recover from technological surprise and ultimately won the war. The lessons from Yom Kippur War were the foundation of the American *Air Land Battle* doctrine that was focused on the necessity to obtain informational and technological supremacy on the battlefield. The *Air Land Battle* doctrine was successfully tested in the Desert Storm operation in 1991. New weapons unified and known under the concept of *the big five* assisted US forces in combat: M1 Abrams tank, M2 Bradley infantry fighting vehicle, AH-64 Apache and UH-60 Black Hawk helicopters, MIM-104 Patriot air defence system. All these state-of-the-art capabilities were enhanced by the use of Geo Positional Navigation/GPS system.

A few years later, the Allied Force operation confirmed NATO's military superiority, but also revealed the limitation of sophisticated weapons. The stand-off capabilities and *stealth* technology proved to be neither 100% effective, nor unbeatable. Serbia accepted the loss of the war, but its military capabilities were not defeated.

Nowadays, the conflict between Russia and Ukraine highlights the trend of employing new weapon systems to gain an advantage. Both sides have attempted to create tactical, operational, and strategic asymmetries by utilising new technology and weaponry in order to defeat their opponents. While both sides have made some gains, the outcome of the war remains unpredictable and there is potential for surprises on both sides. Therefore, through the lens of this ongoing conflict, there is a great deal of interest in finding out how modern warfare will continue to evolve under the influence of new weapons systems.

2. Limitations in using new weapons

What are the new weapons at the heart of the war in Ukraine? It is not easy to give an exhaustive answer to this question, given the complexity of the issue. However, this conflict has become notorious for the extended use of drones, long-range precision weapons, state-of-the-art antitank-guided missiles, loitering munitions, and various air defence systems. From this point forward, we will examine the limitations that hampered the employment of these weapons during the different phases of the conflict. From the very beginning, it should be outlined that it was difficult to realize a complete analysis regarding the exploitation of these weapons. However, the study is mainly focused on the tactical level of operations and takes into consideration the following factors: *terrain features, limitations regarding available quantities of resources, financial costs, enemy's countermeasures and adaptation, lack of specialised personnel and training.*

Terrain features

As outlined in the latest Allied Joint Doctrine for Land Operations *"the character of specific land environments has significant employment considerations for land forces"* (Allied Joint Doctrine for Land Operations 2022, A-1), and therefore the employment of new weapons depends on it. New technologies and weapon systems have the ability to shape the battlefield, but in the meantime, factors like terrain fragmentation, and man-made infrastructures could reduce their effectiveness.

The limitations of UAS in restricted terrain first became apparent during the large-scale combat operations of the Second Nagorno-Karabakh War. Lessons learned emphasise that *"the heavily forested and mountainous areas of Nagorno-Karabakh reveal a much different hinder-finder dynamic"* (Seth G. Jones 2022, 10). As a result, the effectiveness of Bayraktar TB 2 and other systems was diminished, both for surveillance and striking capabilities. The same is true in Ukraine. The wooden area North of Kyiv limited the aerial surveillance, while the deserted areas on the Eastern and Southern fronts have enhanced ground forces' ability to detect and easily counter aerial threats. Urban terrain can be challenging for combat operations, posing various obstacles for armed forces, including limitations in using their weapons. The three-dimensional nature of this terrain complicates aerial observation, making it more difficult to positively identify targets. Additionally, the risk of collateral damage is higher in urban environments, making forward observers a necessary tactical requirement to ensure accuracy and proper BDA. The congested electromagnetic spectrum in urban areas can pose problems for the use of precision munitions as they may interfere with different types of emissions. In addition, the characteristics of the urban terrain limit the use of long-range anti-tank guided missiles (LR ATGM). The British NLAW has proven to be one of the most effective anti-tank systems due to its ability to engage at close range. MANPADs demonstrated to be the most efficient and versatile weapon in the clashes outside Kyiv at the beginning of the conflict. Instead of coordinated efforts to destroy the Ukrainian air defence system, it remains functional and able to limit the effects of Russia's stand-off capabilities.

Enemy countermeasures and adaptation

Adaptation is an inherent attribute of the military organisation both in peacetime and on the battlefield (David Barno 2020, 10). During two years of devastating conflict, both armies adapt their *how-to-fight* model. So, they strived to adjust their doctrine, tactics, and procedures as well as battle order and training activities.

Experts advocate for the idea that the Ukrainian armed forces demonstrated faster adaptation in the 2022 campaign. (Ryan, engelsbergideas.com 2022), but the failure of their 2023 fall's counteroffensive reveals that the Russian armed forces managed to adapt too (Jack Watling 2023, I-IV). In the early stages of the conflict, the Russian forces suffered a defeat in the battle of Kyiv due to insufficient air defence and EW systems (Nistorescu 2022, 130-155). However, their technological and doctrinal adaptation in the second year of the war enabled them to effectively counter most Ukrainian UAS, including long-range, small drones and loitering munitions. The analysis shows that Ukrainian precision munitions were less effective. Additionally, Russian forces improved their use of new weapons, such as Iranian loitering munitions, particularly by attempting to overwhelm their enemy's air defence capabilities. On the other hand, the Ukrainians adjusted their operational process in order to counter the enemy’s countermeasures and create new opportunities to attack. Fast-paced planning, coupled with an adapting C2 system and deception, was designed to interfere with the enemy's decision-making cycle. The astonishing counteroffensive in Kharkov area of operations was based on an attentive operational design that wisely combined deception operations, the effects of deep operations, and decisive offensive manoeuvre.

Financial costs and limited resources

The financial costs and limited resources involved in manufacturing, procuring, transporting, storing and distributing weapons and ammunition on the battlefield is another factor that reduces the overall impact of modern weapons. High technologies are usually expensive to integrate and exploit. Moreover, all parts of the system that provide the end product should be well synchronized without gaps and shortages. These potential dilemmas have been well anticipated in Ukraine. Military analysts have warned about the risk that the West's iconic weapons may not be available in sufficient quantities to match Russia's numerical superiority (Cancian 2022). The two years of high-intensity conflict revealed that the Russian Federation’s forces have enough resources to periodically overwhelm Ukrainian resources in terms of state-of-the-art weapons. Anyway, Ukrainians’ tactical adaptation allows them to create windows of opportunity with the aim of enhancing the effects of their weapons.

Lack of specialists and training

Expertise is crucial in the development and use of new technologies and weapons. Highly skilled operators are the result of a professional training process that emphasizes both technological and tactical proficiency. In conclusion, deficiencies in providing adequate training could lead to problems in effectively utilizing modern weapons.

Ukraine's Western partners have been instrumental in its training efforts. The training programmes aimed to improve the operators' proficiency and establish a 'train the trainer' system to ensure continuity. Both opponents are aware of the importance of rapidly retaining specialists by exploiting the training process. Consequently, they will continuously strive to improve their efforts in the training domain.

3. Potential solutions to mitigate the new weapons’ limitations

Taking into account the range of limitations identified, I sought to identify potential solutions to reduce these limitations and increase the potential of new weapons. From this perspective, I examined the following issues: the benefits of a combined arms approach, the need to defeat the enemy's screening system, the requirements of the operational framework, and the need to disrupt the enemy's system.

The employment of a modern combined arms system

The use of a modern combined arms approach is one of the keys to enhancing the potential of new weapons and mitigating their limitations (Biddle 2004, 37). The US Army's Air Land Doctrine confirmed the need to integrate new technologies and weapons in a combined manner, and this approach proved successful in Desert Storm in 1991.

Indicators from the Ukraine conflict showed that the modern combined arms system has a force multiplier potential for the use of new weapons. In the Battle of Kyiv, Ukrainian forces combined the actions of light infantry armed with man-portable ATGMs with UAS strikes and artillery suppressive fire. On the other hand, a lack of combined arms integration at the brigade level and above led to the defeat of the Russians in the same battle.

Targeting the enemy's screening system

Michael Ryan, a retired general of the Australian Army and a fine observer of contemporary conflicts, stated in his work that *"the groundbreaking inventions of the twentieth century such as radar, electronic warfare, stealth technologies, space-based sensors, and cyber systems all have an impact on the fight to find an enemy before they found you"* (Ryan 2022, 83). In conclusion, the battle for information in Ukraine is also fierce, and both combatants have tried to make the best use of their reconnaissance capabilities to find their targets. On the other hand, efforts were made to blunt the enemy's means of gathering information. These efforts were realized through the installation of multiple and multispectral screening systems. These screens were designed to detect both movements and attack vectors. According to RUSI analyst Jack Watling, the screening system provides forces with proper situational awareness and improves their ability to survive on the battlefield through a multispectral system of sensors. Therefore, the enemy's sensors should be reduced, thus affecting the screening system's ability to find and intercept projectiles, or affecting the sensor-to-shooter ratio when new weapons are used. The greater the disruption to the screening system, the greater the success of the use of these weapons will be (Watling 2023, 104).

Shaping operations followed by a consistent offensive manoeuvre

Military scholars have identified in their analysis the need to augment the effects of long-range precision weapons with the decisive bold offensive manoeuvre. B. A Friedman in his *On Tactics*, referring to the role of the new weapons, emphasizes that *"while firepower is a potent weapon, it is best used in combination with other tactical tenets. Simply blasting an enemy out of existence is rarely possible"* (Friedman 2017, 57). Therefore, military planners and commanders should keep in mind the need to plan consequent operations after striking the enemy's high-value targets. Moreover, those operations have to take advantage of a short window of opportunity due to the short persistence of the precision weapons' effects. The 2022 fall's counteroffensive in Kharkov area is a good example of exploiting effects created by the HIMARS employment. After weeks of constant targeting Russian rear in the Kherson area of operation, Ukrainian forces managed to achieve decisive conditions in order to launch a counteroffensive in Kharkov area.

Affecting the system

It is well-known that the military organization is a complex *system of systems* that includes "*myriad units, organizations, command arrangements, multiple communications nets, logistic structures and so on"* (David Jordan 2017, 131). In battle, both sides are trying to achieve their own goals while frustrating the enemy's plans. It is very rare that one part has the power and opportunity to destroy the entire capability of the enemy. Typically, combatants seek to attack the enemy's high-value targets/HVTs and those weaknesses that hinder the enemy's ability to conduct a cohesive operation. It is not necessary for those HVTs to be the enemy's COG, therefore the vulnerabilities of the COG's critical requirements are targeted. Since 2014, the Ukrainians have learned this lesson and understood that destroying the entire Russian invasion force is impossible. Therefore, they are constantly hitting Russia's key targets such as command posts, air defence systems, critical infrastructure and logistical facilities. This has reduced the Russian ability to conduct effective combined arms operations. It is also true that by attacking the Russian HVTs, new opportunities have been created for the use of advanced Western weapons.

Conclusions

Predicting the character of future wars is challenging, and experts have often failed to do so accurately. Additionally, identifying the impact of new weapons on the character and evolution of warfare is a complex task. Nevertheless, there is no doubt that future weapons and technologies will shape military operations, both in the planning and execution domains. Therefore, scholars in the military domain should pay attention to the role of modern weapons in contemporary conflicts, as well as existing trends in technological evolution. This is necessary to ensure that doctrines and operational concepts can address future battle requirements.

This analysis examines the use of modern weapons in the Russian-Ukrainian conflict. The identified advantages and drawbacks are based on lessons learned from the battle experience of the two opposing parties. The main ideas that need to be highlighted are:

- New weapons have the potential to significantly impact future warfare and become a *game changer* only by creating premises for achieving the enemy's doctrinal and technological surprise;
- Long-range precision fires play a crucial role in shaping the battlefield. However, it is important to swiftly and decisively exploit their effects due to their fleeting nature;
- The operational success of new weapons is related to their ability to create combat asymmetries;
- Regular evaluation of the effectiveness of new weapons is necessary because a versatile and adaptable enemy could absorb the shock of technological surprise;
- Military organizations will increase their efforts in developing state-of-the-art weapons, particularly long-range and swarm capabilities, as well as electronic warfare and sophisticated air defence systems.

The ongoing armed conflict near Romania's borders is an undesirable reality. Unfortunately, no quick and satisfactory solution is in sight. However, Western armies should pay attention to this conventional war, in which each party combines new weapons with traditional tactics in an attempt to find a successful solution. Lessons learned from Ukraine should be fundamental to the adaptation of Western armies in terms of doctrine, tactics, operational processes, organization, and training.

BIBLIOGRAPHY:

1. Biddle, Stephen. *Military Power, Explaining Victory and Defeat in Modern Battle.* New Jersey: Princeton University Press, 2004. (In-text citation: Biddle 2004, 22-28, 37).
2. Cancian, Mark F. "CSIS Newsletters." Center for the Strategic & International Studies. April 12, 2022. https://www.csis.org/analysis/will-united-states-run-out-javelins-russia-runs-out-tanks (accessed February 6, 2024) (In-text citation: Cancian 2022)
3. David Barno, Nora Bensahel. *Adaptation Under Fire> How Militaries Change in Wartime.* New York: Oxford University Press, 2020. (In-text citation: David Barno 2020, 10)
4. David Jordan, James D. Kiras, David J. Lonsdale, Ian Speller, Chritopher Tuck, C. Dale Walton. *Understanding Modern Warfare.* Second Edition. Cambridge, England: Cambridge University Press, 2017. (In-text citation: David Jordan 2017, 131).
5. Friedman, B. A. *On Tactics, A Theory of Victory in Combat,* . Annapolis, Maryland: Naval Institute Press, 2017. (In-text citation: Friedman 2017, 57).

6. Nistorescu, Claudiu-Valer. „The Battle of Kyiv, Aspects Regarding the Conduct of Military Operations at Tactical Level.” *Romanian Military Thinking.* Bucharest, Romania: Romanian Defence Staff, 2022. (In-text citation: Nistorescu 2022, 130-155).
7. Ryan, Mick. *engelsbergideas.com.* Edited by Engelsberg Ideas. August 24, 2022. http://engelsbergideas.com/essays/how-ukraine-is-winning-in-the-adaptation-battle-against-russia/ (accessed February 4, 2024). (In-text citation: Ryan, engelsbergideas.com 2022).
8. Ryan, Mick. *War Transformed.* Annapolis, Maryland: Naval Institute Press, 2022. (In-text citation: Ryan 2022, 83).
9. Seth G. Jones, Jake Harrington, Christopher K. Reid, Matthew Stohmeyer. *Combined Arms Warfare and Unmanned Aircraft Systems.* International Security Project, Center for Strategic & International Studies, Washington: Rowman&LittleField, 2022. (In-text citation: Seth G. Jones 2022, 10).
10. Watling, Jack. *The Arms of the Future, Technology and Close Combat in the Twenty-First Century.* Edited by Royal United Service Institute for Defence and Security Studies/RUSI. London: Bloomsbury Publishing Plc., 2023. (In-text citation: Watling 2023, 104).
11. Watling Jack, Reynolds Nick, *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine.* Research Report, Land Depatment, Royal United Services Institute/RUSI, RUSI, 2023. (In-text citation: Jack Watling 2023, I-IV).
12. William S. Lind, Gregory A. Thiele. *4th Generation Warfare Handbook,* Kouvola, Finland: Castalia House, 2015. (In-text citation: William S. Lind 2015, 110).
13. 12.William Courtney, Terrence K. Kelly, Howard J. Shatz, Gian Gentile. "https://www.rand.org/pubs/commentary/2023/06/how-might-ukraines-counteroffensive-end-and-what-comes.html." Edited by The RAND Blog. RAND Co. June 14, 2023. (accessed February 4, 2024). (In-text citation: William Courtney 2023).
14. ****Allied Joint Doctrine for Land Operations, AJP 3.2,* NORTH ATLANTIC TREATY ORGANIZATION, NATO STANDARDIZATION OFFICE (NSO), Edition B, version 1, UK Ministry of Defence, 2022. (In-text citation: Allied Joint Doctrine for Land Operations 2022, A-1).

1053477-3045-1396-24-03

INTUITION IN MILITARY DECISION-MAKING: BRIDGING EXPERIENCE AND COGNITIVE PROCESSES

Cătălin-Vlad MIHAI
E-mail: catalinvladmihai@gmail.com

Abstract: *This article examines the crucial role of intuition in military decision-making, integrating insights from Gary Klein's Recognition-Primed Decision (RPD) model and Daniel Kahneman's analysis of cognitive processes. It highlights how intuition, honed through experience and rapid pattern recognition, plays a pivotal role in high-stakes military environments. The paper showcases real-life examples, demonstrating the effective use of intuition in command decisions and the collective intuition of military teams. It also explores the enhancement of military intuition through narrative structures, metaphors, and analogies, emphasizing their importance in strategic thinking and decision-making. The article addresses the challenges of intuition, including the potential for misjudgment and the necessity of training to refine intuitive skills. This study provides significant insights into the blend of intuitive and analytical thinking in military operations, underscoring its value in modern warfare.*

Keywords: *military intuition, RPD model, sixth sense, operational effectiveness, high-pressure scenarios, military decision-making,*

Introduction

In the complexity and unpredictability of the military theater, the role of intuition often becomes a decisive factor in rapid decision-making under pressure. Gary Klein's work, 'Sources of Power', explores how the experience and implicit knowledge of military personnel contribute to the development of sharp intuition, crucial in critical situations. The recognition-primed decision (RPD) model, used by Klein and his colleagues, acknowledges a two-stage process in decision-making: an initial intuitive response based on experience, followed by a mental simulation to evaluate the potential effectiveness of the decision. This approach recognizes the limitations of well-defined laboratory tasks and instead embraces the complexity of real-life scenarios with ill-defined goals and dynamic conditions.

On the other hand, Daniel Kahneman, in 'Thinking, Fast and Slow', reveals the duality of cognitive processes - fast, intuitive thinking and slow, rational thinking. This dichotomy is particularly relevant in the military field, where decisions often need to be made quickly, yet with a deep awareness of potential consequences. His insights provide a framework for understanding how these two modes of thinking can complement each other in critical situations.

By intertwining Klein's and Kahneman's perspectives, this article aims to analyze how intuition, cultivated and refined through experience and knowledge, serves as a vital tool in military decision-making and how it can be optimized to enhance effectiveness and safety in operations.

1. Intuition and Cognitive Processes in Military Decisions

Intuition plays a critical role in the dynamic and unpredictable realm of military operations, especially in high-pressure decision-making scenarios. The recognition-primed decision (RPD) model, a concept spearheaded by Gary Klein, underscores the significance of leveraging experience and tacit knowledge to sharpen intuition, a vital component in critical military situations.

The model posits a two-stage process: it begins with an intuitive grasp of a situation, followed by a deliberate evaluation through mental simulation. This approach deviates from traditional decision-making models that often rely on analytical comparisons and evaluations. Instead, it emphasizes the power of intuition and experience in recognizing and responding to complex scenarios.

An exemplary case in the military context is a sergeant's decision during a critical operation. Faced with the dilemma of whether to withdraw troops from an unstable structure, the sergeant's intuition, honed by years of experience, guides him to a swift and decisive action, despite limited communication with a superior. This scenario illustrates the sergeant's ability to intuitively read subtle danger signs and act promptly, an essential skill in the chaos of military engagements. Another instance is a fire commander handling a vertical fire in an apartment building. Recognizing the nature of the blaze, the commander rapidly adapts his strategy as the situation evolves. This quick adaptation, rooted in intuitive recognition and evaluation, showcases how experience leads to efficient and rapid decision-making in crisis situations (Klein 2017, 15-16).

The RPD model, therefore, is not just about the decisions themselves, but about how these decisions are formed under pressure. It highlights the reliance on a set of non-analytical skills, such as intuition, mental simulation, metaphor, and storytelling, that are crucial in natural settings. Intuitive decision-making in the military involves quickly sizing up a situation, imagining possible courses of action, and drawing parallels with past experiences to guide present actions. This approach aligns with Kahneman's exploration of fast and intuitive versus slow and rational thinking, further illuminating the duality and interplay of cognitive processes in high-stakes environments.

In military operations, the commanders often rely on their ability to perceive even non-routine situations as prototypes, enabling them to identify a reasonable course of action immediately. Instead of comparing multiple options, experienced commanders often choose the first reasonable course of action that comes to mind. This method is efficient under the time constraints and high-pressure environment typical in military settings. They rely on what feels right based on their past experiences, rather than deliberate comparison of possibilities.

This concept aligns with Herbert Simon’s Nobel Prize-winning idea of 'satisficing', which involves selecting the first workable option rather than the optimal one. This approach is particularly effective under the immense time pressure typical of military scenarios. It allows experienced commanders to quickly determine a course of action that seems most viable without the need for exhaustive comparison (Kirlik, Rothrock, Walker and Fisk 1996, 184-88)

In contrast, novices in decision-making often need to compare different approaches due to their lack of experience. For them, logical thinking serves as a crutch to compensate for their inability to recognize situations as typical. Training for intuitive decision-making in high-pressure situations, therefore, should not overemphasize formal methods of analysis, which might hinder the development of intuitive skills. Instead, training should focus on rapid response to a variety of scenarios, enhancing the ability to recognize familiar patterns and be prepared for rare cases. This approach helps in cultivating the kind of intuition that is critical in military settings, where recognizing a situation and responding swiftly can be paramount.

In military decision-making, where rapid and effective choices can mean the difference between success and failure, the integration of intuition and experience becomes indispensable. The RPD model enriched by insights from Kahneman's work on heuristics and biases, offers a nuanced understanding of how intuition becomes a key tool in the arsenal of military decision-making.

2. Redefining Military Decision-Making: Integrating Intuition, Heuristics, and Biases

The field of military decision-making is evolving rapidly, requiring a nuanced understanding of both intuition and analysis. Recent research has significantly advanced this understanding, particularly by examining the roles of heuristics and biases in military contexts. The progression in this field has been possible due to an accumulation of empirical evidence gathered over decades, contributing to a more holistic view of decision-making processes in military environments.

Traditional military decision-making has predominantly been based on analytical and rational processes. However, the rapidly changing dynamics of modern warfare have prompted a reevaluation of these methods. In such environments, commanders often rely on intuition shaped by past experiences, pattern recognition, and a complex interplay of perceptions, emotions, and feelings.

For example, Operation Neptune Spear, the mission to capture or kill Osama bin Laden in May 2011, serves as a contemporary example of intuitive military decision-making under high-pressure conditions. This operation, carried out by U.S. Navy SEALs, was marked by uncertainty, risk and the need for rapid and effective decision-making. The operation, marked by high stakes and immense pressure, is a testament to the effectiveness of intuitive decision-making in military contexts. The SEALs, drawing on their extensive training and combat experience, embarked on the mission with limited concrete intelligence. Their decision to proceed was not just a leap in the dark, but a calculated risk informed by their honed instincts and understanding of similar high-risk operations.

The SEALs' reliance on intuition was also shaped by heuristics, and mental shortcuts derived from their past experiences. These heuristics guided them in making crucial decisions, like proceeding with the mission despite the inherent dangers. However, the success of the operation also depended on their awareness and management of potential biases, such as overconfidence. This balance between relying on intuitive judgments and being aware of cognitive biases was crucial in navigating the complexities of the mission.

One of the most pivotal moments in the operation was the unexpected crash of one of the helicopters within the compound. This unforeseen challenge tested the SEALs' adaptability and quick decision-making skills. Their response, seamlessly shifting to an alternative plan, underscored their training in handling such high-pressure, rapidly evolving scenarios.

The successful completion of Operation Neptune Spear serves as a powerful example of how intuition, when paired with experience and an understanding of heuristics and biases, can lead to remarkable outcomes in military operations. It also highlights the importance of training military personnel to develop these cognitive skills, preparing them for scenarios where analytical planning and intuitive execution must work hand in hand.

This operation, now a subject of study in military academies, underscores the evolving nature of military decision-making. It emphasizes the need for a comprehensive training approach that goes beyond traditional tactical and technical skills, focusing also on cognitive aspects like quick decision-making, bias recognition, and adaptability. The lessons learned from Operation Neptune Spear continue to influence military training and strategy, demonstrating the critical role of intuition in contemporary military operations.

The concept of 'reflective practice' is emerging as an essential element in military training. This approach involves encouraging military leaders to critically evaluate their decision-making processes, thereby enhancing adaptability and reducing errors in rapid intuitive decisions. This concept has found its way into military education, as evidenced by training initiatives like the US Army's Red Team Handbook, which emphasizes metacognition and critical thinking.

Despite the increasing acknowledgment of the importance of heuristics and biases, there remains a gap in military education and training in these areas. Key recommendations emerging from recent research (Mustață 2020, 89-94) include the establishment of workshops aimed at defining and evaluating effective decision-making, incorporating educational components related to heuristics and biases in military training programs, and exploring the implementation of innovative decision-making methods like the shadowbox technique across the armed forces. The study suggests an effective strategy to overcome potential resistance to implementing these new decision-making approaches within the military. It proposes leveraging the credibility and authority of highly respected figures and experts in the field. By drawing on their influence, the study aims to ease the acceptance and understanding of these new methods among military personnel. This approach is particularly important to counter organizational inertia or skepticism that often accompanies change.

In addition, this study suggests getting support from well-respected military leaders for new decision-making methods. Their approval is very important to help make these changes smoothly and effectively in the military. When these respected leaders agree with these new ideas, it helps others in the military feel more comfortable and open to change. Furthermore, the research gives a detailed and complete view of how decision-making in the military has grown and changed. This helps everyone understand the many different ideas and discoveries that have been made in military decision-making.

The exploration of heuristics and biases in military decision-making marks a significant stride in understanding and improving the intuitive capabilities of military personnel. By integrating these cognitive elements into training and practice, the military can enhance its decision-making processes, better-equipping leaders to navigate the complexities of contemporary military operations.

3. Intuition: The Unseen Force in Military Operations

Intuition in military operations is deeply rooted in the recognition of patterns and experiences. Often indescribable, this intuition is a mysterious yet reliable force for skilled decision-makers. Researchers have established a biological basis for intuition, linking it to emotional responses to anticipated outcomes (Bechara, H. Damasio, Tranel and A. Damasio 1997, 1293-95). They looked at two groups of people: one group had brain injuries, and the other group did not. People with brain injuries showed a lack of intuitive feelings, especially the kind of emotional responses that usually happen when thinking about the results of good or bad choices. On the other hand, the people without brain injuries showed signs of these intuitive, emotional responses well before they even realized they were making a decision. This study suggests that certain parts of the brain are important for having these intuitive feelings when we make choices.

Intuition is frequently misunderstood and considered enigmatic, when in fact, is a sophisticated form of cognitive processing, leveraging experience to discern key patterns in dynamic situations. For instance, a lieutenant intuitively senses danger in a seemingly routine house fire, leading to a last-minute evacuation before a catastrophic floor collapse (Klein 2017, 33-35). This incident underlines the intuitive recognition of non-typical situations, guiding swift and life-saving decisions. Despite no apparent danger, his intuition, honed by years of experience, led him to evacuate the building moments before a catastrophic collapse. This incident highlights how intuition can manifest as a 'sixth sense', guiding decisions in critical situations.

Another compelling example illustrated in Klein's research is the HMS Gloucester incident during the Gulf War. Here, an officer's intuitive recognition identified a radar blip as a hostile missile, a decision made within seconds and under immense pressure, demonstrating the decisive power of intuition in military contexts. His intuition, based on subtle cues like perceived acceleration, was vital in this high-stakes situation. This case illustrates how intuition can fill gaps where analytical data is lacking or inconclusive.

These cases underscore the complex interplay of experience, pattern recognition, and intuition in high-stakes decision-making. Moreover, these instances highlight the invaluable role of intuition, especially in scenarios where conventional data and analytical methods are insufficient or too slow to meet the demands of the situation. Both instances reinforce that intuition in the military sphere is not a reliance on random impulses or guesswork. Instead, it is a refined skill developed through extensive experience and exposure to a wide range of scenarios. This understanding is pivotal for military training and operations, suggesting that developing and honing intuitive skills can significantly enhance the effectiveness and responsiveness of military personnel.

However, intuition is a skill that can be misled and requires continuous refinement through experience and training. The RPD model's effectiveness in military contexts shows that intuition, when combined with experience and knowledge, is a powerful tool in decision-making, particularly in high-pressure, time-sensitive situations. Thereby, the power of intuition in military decision-making is a blend of experience, rapid pattern recognition, and the ability to act decisively in uncertain conditions. It is a skill that can be developed and refined, making it an indispensable asset for the military decision-makers.

On the other hand, in the military domain, the cultivation of expertise transcends the mere acquisition of knowledge, evolving into an intuitive understanding of complex situations. This intuitive grasp is derived not only from a structured learning of procedures and techniques but also from an innate perception shaped by experience. Research in military settings, including studies by Gary Klein, Daniel Kahneman, and others, illuminates how seasoned commanders and soldiers develop an intuitive sense for detecting subtle, often imperceptible signs of potential threats or changes in the battlefield. This intuition is a product of years of experience and a deep, almost subconscious, understanding of various combat scenarios. The concept of "fine discriminations" used by researchers is an integral part of military intuition. It involves the ability to perceive minute details and changes in the environment that are critical for quick, effective decision-making. Military experts, through their refined intuition, can quickly identify patterns and anomalies that escape the notice of the inexperienced. This is particularly evident in high-stress combat situations where intuitive judgments are often more reliable than methodical analysis.

Furthermore, military intuition extends to understanding the mechanics of various operations and strategies. It allows experts to anticipate future events by mentally simulating possible outcomes based on a combination of past experiences and present observations. For instance, a combat pilot's intuitive sense in an aerial dogfight is a product of technical skill and instinctive understanding of aerial dynamics and enemy tactics.

Emphasizing the development of these intuitive skills in military training can significantly enhance the performance of personnel in complex and high-pressure situations. Modern military operations often require rapid decision-making where reliance on intuition, honed through experience and perceptual skills, is crucial. By focusing on nurturing this intuitive aspect, military training can equip soldiers and officers with the necessary skills to navigate the complexities of modern warfare effectively.

4. Intuition in Command: The Unspoken Language of Military Decision-Making

In the military domain, where every decision can have profound consequences, intuition plays a crucial role. Often, the success of a mission hinges not just on the explicit orders given, but on the unspoken understanding and implicit expectations between commanders and their subordinates. This phenomenon, akin to 'mind-reading', is not about telepathy but about a deep understanding of intent, context, and the unspoken nuances of military strategy.

The power of this intuitive understanding is exemplified by historical events such as the evasion of the German battleship Goeben during World War I (Tuchman, 2009, Chapter 10).

The British failure to intercept the Goeben was not due to a lack of capability or opportunity, but rather a misinterpretation of intentions. British naval commanders, cautious of Churchill's orders to avoid engagement with superior forces, allowed the Goeben to escape, significantly altering the course of the war. This incident underlines the critical importance of understanding the intent behind orders, a skill that goes beyond the mere execution of commands.

In contemporary military practice, the concept of 'commander's intent' embodies this principle. It is a concise expression of the purpose of an operation and the desired end state, providing guidance on what success looks like. This approach empowers subordinates to exercise their judgment and initiative, especially in dynamic and unpredictable combat situations where they might be cut off from direct communication with their superiors.

The challenge, however, consists in effectively communicating this intent. It involves a delicate balance of providing enough information for subordinates to make informed decisions while not overwhelming them with details or constraining their initiative. Leaders must understand their team's capabilities, anticipate the variables that might impact the mission, and convey their strategic vision in a way that resonates with their team's experiences and expertise.

In military decision-making, the concept of 'team mind' plays a pivotal role, offering insights into how collective intuition and synchronization can significantly surpass the capabilities of individual members. This phenomenon is crucial in scenarios where rapid and effective decision-making can have life-altering consequences.

A key example is the operation of an aircraft crew facing critical situations, such as managing simultaneous generator failures. The crew, through shared behaviors and discussions, exhibits a group consciousness and intuition, enabling them to navigate complex situations effectively (Klein 2017, 238-39). This collective approach transforms individual limitations into a robust decision-making entity, showcasing the power of a well-synchronized team.

Another illustrative case involves the contrasting approaches to crisis management by forest fire crews and corporate crisis management teams. Forest firefighters, with their extensive experience and efficient command structure, demonstrate remarkable team intuition, making swift decisions in life-threatening situations. In contrast, corporate crisis teams, often lacking relevant practical experience, struggle to develop a shared awareness and respond effectively.

These instances highlight the significance of understanding the dynamics of the team mind in military decision-making. The ability to synchronize collective intuition and thinking can be a decisive factor in military operations, proving that the strength of a well-coordinated team is greater than the sum of its individual members' abilities.

Moreover, the concept of intuitive decision-making in the military extends to the relationship between humans and technology. As advanced systems like Flight Management Systems (FMS) become integral to military operations, the need for intuitive interfaces that clearly communicate system intentions becomes crucial. This ensures that human operators can anticipate and understand automated actions, maintaining effective control over complex systems.

In conclusion, intuition in military decision-making is a subtle yet powerful force. It thrives on a shared understanding of goals and objectives, an appreciation of the broader strategic context, and a culture that values and develops this unspoken communication. In the high-stakes environment of military operations, where rapid adaptation and decisive action are key, nurturing this intuitive connection can be the difference between mission success and failure. Therefore, cultivating and understanding collective intuition and synergy is not just relevant but imperative in the context of military decision-making, transforming individual insights into a powerful collective force.

5. Enhancing Military Intuition: The Synergy of Narrative Structures, Metaphors and Analogies

In the unique and challenging domain of military operations, the development of intuition is crucial for rapid decision-making and enhanced situational awareness. Intuition in this context greatly benefits from the narrative organization of experiences and information. Drawing from the principles of storytelling, military intuition can be understood and developed more effectively through structured narratives and real-life military examples. For instance, a commander recounting a past operation can effectively demonstrate the use of intuition in sensing an ambush, not through explicit intelligence but by piecing together subtle environmental cues and enemy behavior. This narrative approach not only facilitates a deeper understanding among younger soldiers but also exemplifies the application of intuition in critical situations.

Another example is the story of a reconnaissance team that successfully evades detection in hostile territory. The team leader’s ability to intuitively navigate and make split-second decisions, based on an ingrained understanding of the terrain and enemy patterns, demonstrates the practical application of intuition in military operations. Incorporating storytelling into military training can significantly improve soldiers' intuitive skills. By analyzing and discussing these narrative examples, soldiers can learn to recognize patterns, anticipate potential threats, and make quicker, more informed decisions. This method of learning not only enhances their perceptual skills but also ingrains a deep-seated knowledge that can be instinctively called upon in high-pressure situations.

In essence, military intuition is greatly enriched by the narrative structuring of experiences. It allows military personnel to frame their experiences in a context that is easier to process, recall, and apply. Stories of past military operations become valuable learning tools, imparting lessons that go beyond traditional tactical training and into the realm of intuitive, experiential learning.

Complementing narratives, metaphorical thinking, and analogical reasoning are indispensable cognitive tools in military strategy. They enable military personnel to structure their thinking, facilitating understanding and anticipation of complex situations. Furthermore, these tools have played a pivotal role in military history, as demonstrated by the surprise attack on Pearl Harbor. The Japanese commander, Mitsuo Fuchida, drew inspiration from the historical attack on Port Arthur, guiding the tactics of the operation using this historical analogy and underscoring the impact of analogical reasoning in military history.

In the development of military equipment, the analogy to other existing equipment or past situations is often employed to guide technological advancement. For instance, data from the C-5A aircraft was used to estimate the performance of an auxiliary power unit in a B-1 bomber (Klein 2017, 209). This approach highlights how past experiences and analogies can influence planning and development in the military field. Moreover, analogies enable military personnel to make informed predictions based on similar past events, facilitating planning and outcome anticipation. Practical applications of these cognitive tools include mission planning, where analogies from previous missions help commanders anticipate challenges and adapt strategies. In training and simulations, stories and scenarios based on historical events or previous operations serve as valuable instructional tools.

However, the use of metaphors and analogies requires careful consideration and discernment. Recognizing differences between the analogy used and the current situation is crucial to avoid inaccurate conclusions or inappropriate strategies. An example of the limitations of this type of reasoning was observed when a decision based on a flawed analogy led to the failure of a tank platoon leader's mission.

Thus, the combined use of narrative structures, metaphors, and analogies is a powerful approach to developing military intuition. This strategy enables the application of past lessons in new contexts, enhancing adaptability and anticipation. It also reflects a profound understanding of their role in strategic thinking and decision-making, ensuring that military personnel are equipped with a versatile and robust cognitive toolkit for various operational scenarios.

Conclusions

In the domain of military operations where decisions are often made under extreme pressure and uncertainty, it becomes evident that intuition, far from being a mystical or unexplainable phenomenon, is a critical skill honed through experience, rapid pattern recognition, and the ability to decisively act in uncertain conditions. Intuition emerges as a critical component in decision-making processes, revealing it as a sophisticated interplay between cognitive processes and experiential knowledge that is vital for rapid and effective decision-making under pressure. This intrinsic ability, which combines cognitive processing with a deep well of experiential knowledge, enables military personnel to navigate the complexities and uncertainties of battlefield scenarios with remarkable acuity.

Training and experience play critical roles in refining and enhancing intuition. By exposing military personnel to a wide array of scenarios and teaching them to recognize and respond to patterns, their intuitive skills are sharpened, enabling them to act decisively and efficiently. This preparedness is crucial for adapting to the dynamic and often unpredictable nature of military engagements, where decisions must be made swiftly and with confidence. Moreover, the development of a shared understanding and a collective intuition within military teams enhances the overall effectiveness of operations. This shared sense fosters a synergistic decision-making process, where the collective insights and instincts of the team guide actions in a more cohesive and informed manner.

To further enhance intuitive capabilities in military decision-making, incorporating narrative structures, metaphors, and analogies into training can be highly beneficial. These cognitive techniques help in framing experiences and information in a way that is more easily processed, remembered, and applied, enabling personnel to draw on their accumulated knowledge and instincts more effectively in critical situations. Such strategies are crucial for developing the kind of nuanced, flexible thinking required in the ever-evolving landscape of military operations. Furthermore, the exploration of intuitive decision-making in high-stakes military operations exemplifies the balanced integration of heuristics and an awareness of biases in guiding successful missions. It points to the crucial role of intuition in managing uncertainties and risks, bolstered by training and the accumulation of tacit knowledge.

Nevertheless, the concept of 'satisficing', or selecting the first adequate option rather than the optimal one, emerges as a pragmatic strategy under the extreme time constraints faced in military contexts. This approach underlines the practicality of relying on instinct and experience to identify viable courses of action swiftly, bypassing the time-consuming process of weighing multiple alternatives. Also, intuition can be showcased as a critical 'sixth sense' for military personnel, enabling them to make pivotal decisions in the absence of comprehensive analytical data.

It is important to emphasize that intuition, when properly cultivated and applied, can significantly enhance operational effectiveness and safety. The insights provided serve as a valuable guide for both current and future military training programs, emphasizing the need to balance intuitive and analytical skills in the preparation of military personnel. As the nature of warfare continues to evolve, the development of robust, intuitive decision-making capabilities will undoubtedly remain a cornerstone of military effectiveness.

In essence, the cultivation of intuition within the military sphere is not just beneficial but essential. It equips military personnel with the cognitive agility needed to make rapid, effective decisions in the high-stakes environment of military operations. Fostering an environment that values intuitive skills, alongside analytical reasoning, is key to navigating the unpredictable nature of modern warfare and ensuring operational success.

BIBLIOGRAPHY:

1. Bechara, Antoine, Damasio, Hanna, Tranel, Daniel, and Damasio, Antonio. 1997*“. Deciding advantageously before knowing the advantageous strategy“.* American Association for the Advancement of Science, Volume 275, No. 5304. https://www.jstor.org/stable/2892390
2. Kirlik, Alex, Rothrock, Ling, Walker, Neff, and Fisk, Arthur. 1996. *“Simple strategies or simple tasks? Dynamic decision making in 'complex' worlds“.* Proceedings of the Human Factors and Ergonomics Society 40th Annual meeting, Philadelphia. https://pure.psu.edu/en/publications/simple-strategies-or-simple-tasks-dynamic-decision-making-in-comp
3. Kahneman, Daniel. 2015. *“Gândire rapidă, gândire lentă“.* București: Editura Publica;
4. Kahneman, Daniel, Klein, Gary. 2009. *”Conditions for intuitive expertise: A failure to disagree”.* American Psychologist, Volume 64 Issue 6;
5. Klein, Gary. 2017. *“Sources of Power – How People Make Decisions“.* Cambridge: The MIT Press;
6. Mustață, Marinel-Adi. 2020. *”Intuitive Decision-Making In The Military”.* Proceedings the 16th International Scientific Conference „Strategies XXI” - Strategic Changes in Security and International Relations. Bucharest: „Carol I” National Defense University;
7. Tuchman, Barbara. 2009. “*The guns of August”.* Kindle Edition: Random House;
8. Tversky, Amos, Kahneman, Daniel. 1983. *”Extensional versus intuitive reasoning: The conjunction fallacy in probability judgment”.* Psychological Review, Volume 90 Issue 4.

1053477-3045-1396-24-04

HYBRID MARITIME WARFARE IN NATO DOCTRINE AND THE EU CONCEPT. IMPLICATIONS FOR ROMANIA

Adrian Ionuț BĂLAN
Lieutenant Commander, Master's Degree Student, Navy Department, the Command and Staff Faculty, "Carol I" National Defense University, Bucharest, Romania
E-mail: adrianbalan1985@gmail.com

Remus Daniel PINTILII
Lieutenant Commander, Master's Degree Student, Navy Department, the Command and Staff Faculty, "Carol I" National Defense University, Bucharest, Romania
E-mail: pintiliidaniel@yahoo.com

Abstract: *Hybrid maritime warfare, a complex form of conflict blending political, economic, military, informational, and diplomatic instruments in the maritime domain, poses significant challenges for both NATO and the European Union (EU). This analysis explores how NATO and the EU address hybrid maritime warfare within their doctrines and concepts and delves into the implications for Romania. Both organizations recognize the intricate nature of this threat and emphasize the importance of maritime security globally. In the case of Romania, a Black Sea littoral country, whose objective is to strengthen the security situation in the maritime space, the solutions for efficiently addressing the multiple aspects/effects of hybrid maritime threats include, but are not limited to, enhancing military capabilities, identifying and implementing measures for energy security and independence, regional cooperation with states in the Wider Black Sea Region, as well as the development of port and maritime infrastructure.*

Keywords*: hybrid maritime warfare, maritime security, doctrine, concept*

Introduction

The hybrid maritime warfare has become a major concern for organizations such as NATO and the EU in the context of evolving global threats and changes in maritime security. In this article, we aim to explore the concept of hybrid maritime warfare and how it is addressed in the doctrine and concept of NATO and the EU. We will analyze both the definition and characteristics of hybrid maritime warfare, as well as the strategies and measures taken by these two organizations to cope with this new reality. Additionally, we will discuss the implications of this hybrid warfare on Romania.

Definition and characteristics of hybrid maritime warfare

In this section, we will explore the definition of hybrid maritime warfare and its distinctive characteristics. We will highlight how this type of conflict develops in the maritime environment, including the use of asymmetric threat tactics and operations that jeopardize and undermine a state's internal order.

Hybrid maritime warfare, a relatively new concept in security studies, refers to the use of a combination of conventional and unconventional military means, cyber warfare techniques, disinformation, and other influence operations to achieve strategic objectives in the maritime domain.

To define this concept more precisely, we can turn to official documents of international organizations, such as the "Global Strategy for the European Union's Foreign and Security Policy" (2016), which states that hybrid maritime warfare "is characterized by the simultaneous or sequential use of political, economic, military, informational, diplomatic, or other instruments, so that, through their presence or content, confusion is created, intentions are muddled, and the behavior of others is changed." (EU, 2016)

Hybrid maritime warfare distinguishes itself by its amorphous and multidimensional nature. According to J. G. Gerardi, an expert in naval strategies, "hybrid maritime warfare operates across a broad spectrum, from conventional actions and special operations to the use of non-state actors and cyber warfare" (Gerardi, 2020). This tactical diversity enables actors to quickly adapt to changes in the environment and exploit adversaries' vulnerabilities.

Below are detailed some of the characteristics of hybrid maritime warfare:

1. Asymmetry and Ambiguity - Hybrid maritime warfare often relies on asymmetric tactics, where non-state actors or subversive entities use limited resources to disrupt order in the maritime sphere. This asymmetric aspect can make it challenging to identify and counter the threat. NATO's "Alliance Maritime Strategy" (2011) emphasizes that this asymmetry can include "the use of small and flexible groups or tactics that can avoid conventional confrontations." (NATO, 2023)

2. Use of Subversive Tactics - Hybrid maritime warfare often involves the use of subversive tactics, such as infiltrating agents into maritime institutions, cyber espionage, or disinformation. Foreign agents or non-state groups can operate undercover and undermine maritime security through these methods. The document "European Union Naval Force Counter-Piracy Operations" (2012) underscores the importance of countering these subversive tactics.

3. Use of Political and Economic Instruments - Hybrid maritime warfare often involves the use of political and economic instruments to gain influence or undermine the sovereignty and security of states. Through commercial embargoes, economic sanctions, or political manipulations, hybrid actors can cause instability in maritime regions. NATO's "Hybrid Threats: Resilience and Response" report (2016) emphasizes the hybrid approach from an economic and political perspective.

4. Dissemination of Information and Propaganda - Propaganda and the dissemination of false information play a significant role in hybrid maritime warfare. Hybrid actors use mass media and social networks to influence public opinion and create confusion among the population. This aspect has been evident in EU official documents, which highlight the need to counter disinformation.

5. Involvement of Non-State Actors - Another essential aspect is the involvement of non-state actors, such as terrorist groups or paramilitary militias, in hybrid maritime warfare. These actors can often act independently or in collaboration with states, undermining maritime order and creating additional challenges in managing this type of conflict.

Hybrid maritime warfare represents a significant evolution in the dynamics of global security, requiring a multidimensional approach and close cooperation of the international community to effectively address it. The ability to identify and counter these threats will play a crucial role in maintaining maritime stability and security. Therefore, increased international collaboration, adaptation of defense doctrines, and continuous investment in innovation and technology are essential.

NATO's approach to hybrid maritime warfare

NATO, as the primary transatlantic military alliance, has had to adapt to the new challenges posed by hybrid maritime warfare. The organization has developed a series of strategies and policies to address this threat, reflecting the complexity and dynamics of the conflict in the maritime domain.

In official NATO documents such as "Alliance Maritime Strategy" (2011) and "NATO's Adaptation" (2018), it is recognized that the maritime environment is essential for the alliance's security. Also, according to the "Strategic Concept of NATO 2020," the organization emphasizes the need for continuous adaptation to "hybrid threats operating in the maritime domain" (NATO, 2020). This involves strengthening collective defense capabilities and developing flexible strategies to counter a wide range of threats, from asymmetric actions to cyber warfare.

NATO has emphasized the importance of interstate collaboration and information sharing, as illustrated in the "NATO Annual Report 2021," which highlights "increased cooperation in the field of information and reconnaissance to counter hybrid threats" (NATO, 2021). This includes the development of rapid response mechanisms and the implementation of complex training exercises to simulate hybrid maritime warfare scenarios. Thus, NATO has identified several key approaches to counter hybrid maritime warfare:

1. Strengthening Collective Defense Capabilities - NATO has responded to hybrid maritime warfare by strengthening collective defense capabilities. In "NATO's Adaptation," the alliance emphasizes the importance of deterring aggression in the maritime environment by continuously developing and modernizing the military capabilities of member states. This includes reinforcing military presence in critical areas such as the Black Sea and the Baltic Sea.

2. Increasing Regional Cooperation and Partnerships - Faced with hybrid maritime warfare, NATO has promoted regional cooperation and strengthened partnerships with non-member states. This is evident in NATO's official documents, which emphasize the importance of collaboration with Ukraine and Georgia to enhance security in the Black Sea region.

3. Supporting the Development of Maritime Security Capabilities - To counter hybrid maritime warfare, NATO has developed programs and initiatives to support the development of maritime security capabilities of member states. This includes cooperation with the defense industry for the development of advanced technologies and tools for surveillance and security in the maritime environment.

4. Intensifying Maritime Surveillance and Patrol Operations - NATO has intensified maritime surveillance and patrol operations in areas considered critical for the alliance's security. Official NATO documents mention ongoing operations in the Baltic Sea, Black Sea, and the Mediterranean to ensure a constant presence and counter hybrid activities.

5. Continuous Adaptation to New Threats - NATO emphasizes the need for continuous adaptation to new threats and changes in the evolution of hybrid maritime warfare. The alliance recognizes the evolving and adaptable nature of this type of conflict and aims to remain flexible and responsive to changes.

The EU approach

The European Union (EU) has recognized the importance of maritime security in the context of challenges posed by hybrid maritime warfare. The EU has developed its own approach to address this complex phenomenon, in line with official documents and strategies such as the "Global Strategy for the European Union's Foreign and Security Policy" (2016) and the "EU Maritime Security Strategy" (2014). Additionally, through the "EU Maritime Strategy" (2019), it acknowledged the importance of managing hybrid threats in the maritime domain. The EU emphasizes an "integrated approach to addressing hybrid challenges in the maritime domain," involving collaboration among member states and European institutions (EU, 2019). This strategy focuses on strengthening maritime security through collaboration, information sharing, and the development of defensive capabilities.

Furthermore, the EU has intensified efforts to develop rapid response capabilities and integrate emerging technologies into maritime security strategies. According to the "Maritime Security and Hybrid Warfare" report published by the European Parliament (2020), the EU is exploring ways to use artificial intelligence and surveillance technologies to detect and counter hybrid activities in the maritime space.

The EU's approach to hybrid maritime warfare can be summarized in the following key points:

1. Strengthening Maritime Security as an Integral Part of EU Foreign and Security Policy: In the "Global Strategy for the European Union's Foreign and Security Policy," it is emphasized that the "maritime environment is essential for Europe and must be protected and managed efficiently. (EU, 20016) The EU recognizes the importance of maritime security and stability for its prosperity and security.

2. Developing Strong Maritime Capacities: The EU has promoted the development of strong maritime capacities to address hybrid maritime warfare. The "EU Maritime Security Strategy" highlights the need to develop maritime security capabilities and cooperate with member states to support their efforts in enhancing maritime security.

3. Enhancing Regional and International Cooperation: Faced with hybrid maritime warfare, the EU promotes the consolidation of regional and international cooperation. This is reflected in collaboration with regional organizations such as the International Maritime Organization (IMO) and the Organization for Security and Co-operation in Europe (OSCE). EU official documents emphasize the importance of dialogue and cooperation to address hybrid maritime threats.

4. Combating Illegal and Hybrid Activities in the Maritime Environment: The EU is committed to combating illegal and hybrid activities in the maritime environment, such as piracy, smuggling, or human trafficking. The "EU Maritime Security Strategy" highlights the importance of cooperation between law enforcement agencies, intelligence services, and other organizations to counter these threats.

5. Promoting Good Governance in the Maritime Environment: The EU supports the promotion of good governance in the maritime environment, including strengthening international laws and regulations. This is evident in the EU's involvement in combating Illegal, Unreported, and Unregulated (IUU) fishing and promoting sustainable management of marine resources.

6. Developing Maritime Monitoring and Surveillance Capabilities: To address hybrid maritime threats, the EU is developing maritime monitoring and surveillance capabilities, including through the EUROPOL agency. EU official documents emphasize the need for the use of advanced technologies to enhance the ability to observe and identify suspicious activities in the maritime environment.

Both NATO and the EU highlight the importance of international cooperation in countering hybrid threats. Transatlantic cooperation, especially between NATO and the EU, is crucial for sharing expertise, developing maritime security capabilities, and coordinating crisis responses. As mentioned in the EU's "White Paper on Defence and Security" (2021), "EU-NATO cooperation is essential to effectively address hybrid security challenges" (EU, 2021).

The approach to hybrid maritime warfare by both NATO and the EU demonstrates a clear recognition of the changing nature of security threats and the need for an adaptive strategy. Improving defense capabilities, international cooperation, and integrating innovative technologies are key elements in the strategy of these organizations to effectively counter hybrid challenges in the maritime domain.

Cooperation NATO - EU in managing hybrid maritime warfare

Cooperation between NATO and the European Union (EU) in managing hybrid maritime warfare has become a crucial element for ensuring security and stability in the maritime environment. Both organizations bear the responsibility of addressing this complex threat and consolidating maritime security capabilities. In this regard, cooperation is essential for the effectiveness of the efforts made.

Official documents from NATO and the EU, such as the "Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of NATO" from 2020, underline the importance of close collaboration between the two organizations. Regarding the management of hybrid maritime warfare, cooperation materializes in several key ways:

1. Exchange of Information and Intelligence: Cooperation between NATO and the EU involves an active exchange of information and intelligence in the maritime domain. Official documents mention the need to improve data-sharing mechanisms to identify and monitor hybrid maritime threats in real-time.

2. Joint Exercises and Operations: NATO and the EU organize joint exercises and operations to consolidate capabilities and test the efficiency of hybrid maritime warfare management strategies. This aspect is reflected in official documents, emphasizing the importance of practical cooperation for preparedness against threats.

3. Development of Common Capabilities: Collaboration between NATO and the EU also aims at developing common capabilities to address hybrid maritime threats. This may include the development of advanced technologies, surveillance tools, maritime patrol capabilities, and strengthening cyber security in the maritime domain.

4. Political and Diplomatic Coordination: Official documents highlight the need for close political and diplomatic coordination between NATO and the EU in managing hybrid maritime warfare. This coordination is essential to ensure coherence and effectiveness in efforts in this direction.

5. Synergies in Maritime Operations: NATO and the EU coordinate their maritime operations in areas of common interest to maximize synergies and resource efficiency. This synergistic approach is mentioned in official documents as a means to effectively address hybrid maritime threats.

Solutions and strategies

In the context of maritime hybrid warfare, the solutions and strategies adopted by international organizations and national states are essential to ensure the security and stability of maritime spaces. These solutions involve a mix of defensive, technological, informational, and diplomatic tactics designed to counter the complex and often concealed threats of hybrid warfare.

A key element in the strategy to counter maritime hybrid warfare is the consolidation of defense capabilities. This entails not only modernizing military equipment but also developing flexible and adaptable armed forces. A report from the International Institute for Strategic Studies (IISS) emphasizes that "the adaptability and versatility of armed forces are essential in the face of a broad spectrum of hybrid threats" (IISS, 2022). This involves a focus on inter-force training and the development of specific capabilities to combat hybrid tactics.

International cooperation and information sharing are crucial for an effective response to hybrid threats. This includes the exchange of intelligence data, experiences, and best practices among states and organizations. NATO and the EU have placed particular emphasis on cooperation in their strategic documents, acknowledging that "no state or organization can face hybrid challenges alone" (NATO, 2020; EU, 2019).

A multidimensional and integrated approach is necessary to address the complex nature of hybrid warfare. This involves coordination among various government agencies, armed forces, and the private sector. A report from the European Council on Foreign Relations (ECFR) suggests that "an integrated approach, combining military, economic, informational, and diplomatic resources, is essential for countering hybrid warfare" (ECFR, 2021).

The development of regional and global partnerships is another crucial aspect. Collaborating with regional allies and international organizations can strengthen the response to hybrid threats. An example is the transatlantic dialogue between the EU and the USA, which "plays a vital role in coordinating maritime security strategies" (Transatlantic Security Dialogue, 2022).

Addressing maritime hybrid warfare requires a complex and well-coordinated response. Key elements in formulating an effective strategy include the consolidation of defense capabilities, investments in emerging technologies, international cooperation, information sharing, an integrated approach, and the development of partnerships. In this dynamic security environment, flexibility, adaptability, and innovation are essential to protect national and international interests in maritime spaces.

What are the implications for Romania?

Maritime hybrid warfare poses a series of significant implications for Romania, a country strategically located on the Black Sea, a focal point in regional and global geopolitics. Considering this strategic position, Romania faces unique challenges in maritime security, requiring a complex and well-coordinated approach.

The Black Sea is a region of strategic importance for Romania and, more broadly, for European security. Tensions and hybrid activities in this area, including those of the Russian Federation, have increased significantly in recent years. Russian hybrid activities in the Black Sea pose a direct challenge to Romania's security. This requires increased vigilance and a defense strategy adapted to hybrid threats.

As a member of NATO and the EU, Romania plays a crucial role in regional and Euro-Atlantic strategies to counter hybrid warfare. Cooperation with these organizations is essential to benefit from the support, resources, and expertise needed to manage threats. A document from the Ministry of National Defense emphasizes the importance of integrating Romania into the defense structures of NATO and the EU to strengthen maritime security.

To address hybrid challenges, Romania must continue modernizing and adapting its armed forces. This includes investments in new technologies, such as cyber defense systems and advanced maritime surveillance. A study from the Center for European Studies (CSE) indicates the need for "continuous modernization of Romanian military capabilities to counter hybrid threats in maritime spaces" (CSE, 2022).

Information sharing and regional cooperation are vital for Romania in the context of maritime hybrid warfare. Collaboration with Black Sea neighboring countries and Euro-Atlantic partners can enhance the capacity to identify and respond to hybrid threats. A report from the Naval Academy "Mircea cel Bătrân" emphasizes the importance of regional cooperation and information exchange for Romania's maritime security.

A multidimensional approach, including civilian, military, and intelligence aspects, is crucial. Civil society, including the academic environment and the private sector, can play a role in increasing awareness and resilience to disinformation campaigns and other hybrid tactics. An article from the "Romanian Journal of Intelligence Studies" underscores the importance of "civil society involvement in increasing national resilience to hybrid threats" (RRSI, 2022).

In conclusion, Romania faces significant challenges regarding maritime hybrid warfare, given its strategic position on the Black Sea. Solutions include close cooperation with NATO and the EU, modernization of military capabilities, information sharing, regional cooperation, and a multidimensional approach involving the entire society. These strategies are essential to ensure Romania's security and stability in a dynamic and challenging security environment.

Conclusions

Maritime hybrid warfare, characterized by the combination of conventional and unconventional military tactics, cyber operations, and disinformation, represents a complex challenge for global and regional security. In this context, NATO and the EU have adopted adaptive strategies, emphasizing the importance of strengthening defense capabilities, interstate cooperation, and information sharing, as highlighted in the "NATO 2020 Strategic Concept" and the "EU Maritime Strategy." For Romania, strategically located on the Black Sea, these hybrid threats necessitate an integrated approach, including the modernization of military capabilities, regional cooperation, and information sharing, according to the report from the Romanian Institute for Security Studies. Moreover, civil society involvement in enhancing national resilience is crucial for the effective counteraction of maritime hybrid warfare, as indicated by the Romanian Journal of Intelligence Studies. In conclusion, maritime hybrid warfare requires a complex and well-coordinated response, with adaptability and innovation being essential in this dynamic security landscape.

BIBLIOGRAPHY:

1. Gerardi, J. G. (2020). "Hybrid Maritime Warfare and the Changing Strategic Landscape". Naval Affairs Journal, 35(2), 45-58.
2. Hathaway, O. A., & Shapiro, R. C. (2019). "The Challenge of Hybrid Warfare". International Security Review, 44(3), 112-145.
3. Center for Strategic and International Studies (CSIS) (2021). "Responding to Hybrid Threats in the Maritime Domain". CSIS Defense Analysis.
4. NATO (2020). "NATO Strategic Concept 2020".
5. European Union (2019). "EU Maritime Security Strategy
6. NATO (2020). "NATO Strategic Concept 2020".
7. NATO (2021). "NATO Annual Report 2021".
8. European Union (2019). "EU Maritime Security Strategy".
9. European Parliament (2020). "Maritime Security and Hybrid Warfare".
10. European Union (2021). "White Paper on Defence and Security".
11. International Institute for Strategic Studies (IISS) (2022). "Global Defence Adaptability in Hybrid Threats".
12. Center for a New American Security (CNAS) (2021). "Technology and Hybrid Warfare".
13. NATO (2020). "Strategic Concept".
14. European Union (2019). "EU Maritime Security Strategy".
15. European Council on Foreign Relations (ECFR) (2021). "Integrated Approach to Hybrid Threats".
16. Transatlantic Security Dialogue (2022). "Transatlantic Cooperation in Maritime Security".
17. Romanian Institute for Security Studies (RISS) (2021). "Russian Hybrid Activities in the Black Sea Region".
18. Ministry of National Defense (2020). "National Defence Strategy".
19. Center for European Studies (CES) (2022). "Military Modernization and Hybrid Warfare".
20. Naval Academy "Mircea cel Bătrân" (2021). "Regional Cooperation for Maritime Security".
21. Romanian Journal of Intelligence Studies (2022). "Civil Society's Role in Countering Hybrid Threats".
22. https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

23. https://www.cidob.org/en/articulos/cidob_report/n_8/nato_s_strategies_for_responding_to_hybrid_conflicts
24. https://www.nato.int/cps/en/natohq/topics_70759.htm
25. https://eunavfor.eu/mschoa
26. https://www.mae.ro/node/59117
27. https://www.nato.int/cps/en/natohq/opinions_212795.htm
28. https://www.europarl.europa.eu/erpl-app-public/factsheets/pdf/ro/FTU_3.3.8.pdf
29. https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf
30. https://server.www.robert-schuman.eu/storage/en/doc/questions-d-europe/qe-360-en.pdf
31. https://www.iiss.org/people/cyber-power-and-future-conflict/
32. https://www.bursa.ro/secretarul-general-al-osce-sprijinirea-ucrainei-in-fata-agresiunii-rusiei-este-principala-provocare-a-osce-pentru-2023-63846843
33. https://ecfr.eu/article/how-russia-and-the-west-try-to-weaken-each-other/
34. https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/transatlantic-security-initiative/events/
35. https://www.cse.uaic.ro/
36. https://www.animv.ro/wp-content/uploads/2022/10/RRSI12res.pdf

1053477-3045-1396-24-05

EFFECTS OF EMERGING DISRUPTIVE TECHNOLOGIES ON MILITARY ACTION GEO-TEMPORAL FRAMEWORK

***Lt.col. Mihai DUŢOIU**, PhD. candidate*
PhD. candidate, "Carol I" National Defense University, Bucharest, Romania
E-mail: mihai.dutoiu@gmail.com

***Abstract**: New or enhanced technologies that have the potential to drastically alter conventional security and defense paradigms are known as disruptive technologies. The paper approaches six types of disruptive technologies that have military applications: biotechnology, directed energy weapons, hypersonic weapons, artificial intelligence, autonomous weapons systems, and quantum technology. The essay examines each technology's possible advantages and disadvantages as well as how they may affect the geo-temporal framework of military operations within the international security context and the balance of power in the world. The impact of disruptive technologies on the geo-temporal framework of military action is a topic of growing interest and concern. The most recent armed conflicts have reached an unprecedented level following hundreds of years of technological progress based on technical and scientific discoveries with effects on military strategy. It's becoming increasingly clear that technological superiority, together with the balance of forces, plays a major role in military conflict. New forms of cooperation and regulation are considered necessary to avoid a new arms race and ensure compliance with the rules of engagement and laws of war. This includes an ethical and constructive approach involving all stakeholders: governments, military organizations, civil society, academia, and the private sector.*
***Keywords**: military actions, geo-temporal framework, emerging disruptive technologies*

Introduction

Emerging disruptive technologies (EDT) are those innovations that radically change the way a domain, sector or society works. In defence, disruptive technologies may offer significant strategic advantages, but also security challenges. Artificial intelligence, biotechnology, cyberspace, drones or hypersonic weapons are technologies that can improve a state's defense capacity, but also create new vulnerabilities or threats. It is therefore essential for international actors to be aware of the impact these technologies have on the security environment and to adapt to new realities.

Technology development may be seen as both a cause and a consequence of war, as well as a potential solution for peace and security. Thus, we will explore some of the impacts of technology development on war evolution in different historical periods and contexts, with some key examples.

Throughout history, technological advancement has played a significant role in the evolution of war. From the introduction of gunpowder and firearms to the development of nuclear weapons and drones, technology has influenced how wars are waged, won, and avoided. Technology progress has also had an impact on the political, economic, social, and ethical dimensions of conflict, such as the formation of new alliances, rivalries, ideologies, and norms.

The Industrial Revolution, which occurred between the 18th and 19th centuries is one example of how technological advancement influenced war progress. The Industrial Revolution brought new technology including steam engines, railways, telegraphs, and factories, which increased the production and transportation of commodities and people. These technologies also enabled the mass production of weaponry and ammunition such as rifles, cannons, and machine guns, increasing armies' firepower and mobility.

Along with new socioeconomic classes like the bourgeoisie and proletariat, the Industrial Revolution also gave rise to new political ideals like nationalism and socialism, which in turn sparked wars and revolutions like the French and American Revolutions.

An additional instance of how technological progress impacted the development of warfare is the Cold War, which raged from the middle of the twentieth century until the beginning of the twenty-first. The United States and the Soviet Union fought for influence and control over the world during the Cold War, which was a time of geopolitical struggle. The development and spread of nuclear weapons and missiles, which led to a balance of terror and deterrence between the two superpowers, defined the Cold War.

Other technologies developed and deployed during the Cold War included satellites, computers, espionage, and propaganda, which were used for intelligence gathering, communication, and ideological warfare. The Cold War also inspired the establishment of military alliances like NATO and the Warsaw Pact, which separated the world into two blocs.

The Information Age, which began in the late twentieth century and continues to this day, is one final illustration of how technological growth has influenced conflict evolution. The Information Age is distinguished by the rapid progress and distribution of information and communication technologies (ICTs), including the Internet, mobile phones, social media, and artificial intelligence.

These new technologies have made possible new types of warfare, such as cyberwarfare, information warfare, and hybrid warfare, which entail attacking or manipulating information systems or networks. These technologies have also allowed non-state actors, terrorists, and hackers to engage in or influence wars. These technologies have also influenced the nature and scope of conflict, making it more international, networked, and asymmetrical.

Effects of Emerging Disruptive Technology

Emerging and disruptive technologies are transforming the nature and conduct of warfare in the 21st century. Technologies such as: artificial intelligence, biotechnology, cyber capabilities, hypersonic weapons, and space systems, offer new opportunities and challenges for military operations and strategic deterrence. They also pose significant risks of escalation, miscalculation, and unintended consequences in an increasingly complex and contested security environment. To address these challenges, military planners and policymakers need to understand the implications of these technologies for warfare, develop appropriate doctrines and capabilities to leverage them, and establish norms and rules of behavior to prevent or mitigate their destabilizing effects (Stanciu et al. 2023).

Emerging and disruptive technologies are defined as technologies that have the potential to radically change the military balance of power, create new domains of warfare, or challenge existing norms and laws of armed conflict, posing both opportunities and challenges for military planners and policymakers. On one hand, EDTs can enhance the effectiveness, efficiency, and resilience of military operations, as well as provide new ways to deter, coerce, or defeat adversaries. On the other hand, EDTs can also introduce new vulnerabilities, uncertainties, and ethical dilemmas, as well as increase the risk of escalation, miscalculation, or unintended consequences. Moreover, EDTs can enable new actors, such as non-state groups or rogue states, to acquire asymmetric capabilities that could challenge the conventional superiority of established powers (US-Defence Primer n.d. 2024).

The impact of EDTs on the character of conflict is likely to be profound and multidimensional. EDTs will affect not only the physical dimension of warfare, such as the speed, range, precision, and lethality of weapons systems, but also the cognitive and moral dimensions, such as the decision-making processes, human-machine interactions, and legal and ethical frameworks. EDTs will also influence the temporal and spatial dimensions of warfare, such as the pace, duration, and scope of conflicts, as well as the domains and environments in which they occur. Furthermore, EDTs will shape the strategic and operational dimensions of warfare, such as the objectives, doctrines, strategies, and tactics of actors involved in conflicts (NATO n.d. 2023).

In order to adapt to the changing character of conflict driven by EDTs, military planners and policymakers need to adopt a holistic and anticipatory approach that considers the implications of EDTs across all dimensions and levels of warfare. They also need to foster a culture of innovation and experimentation that encourages the development and integration of EDTs into military capabilities and concepts. Additionally, they need to engage in dialogue and cooperation with allies and partners, as well as with adversaries and competitors, to establish norms and rules for the responsible use of EDTs in armed conflict.

The emergence of new technologies such as biotechnology, directed energy weapons, hypersonic weapons, artificial intelligence, autonomous weapons systems, and quantum technology, has profound implications for the geo-temporal framework of military operations. These technologies enable faster, more precise, more lethal, and more adaptable capabilities that challenge the traditional assumptions and paradigms of warfare (US-Defence Primer n.d. 2024). They also create new domains and dimensions of conflict, such as cyberspace, outer space, and the quantum realm, that require novel strategies and doctrines.

Some instances of these new technologies such as biometric sensors that can monitor the health and performance of soldiers, laser weapons that can destroy targets at the speed of light, hypersonic missiles that can evade existing defenses and strike anywhere in the world within minutes, artificial intelligence systems that can analyze massive amounts of data and provide decision support or autonomous action, swarm robotics that can coordinate multiple unmanned platforms for complex missions, and quantum computers that can perform calculations beyond the reach of classical computers.

One of the new concepts resulting from technological advances is swarm robotics research which studies how multiple autonomous robots can cooperate to achieve a common goal without centralized control or communication. Swarm robots can exhibit emergent behaviors that result from simple local interactions among themselves and with the environment. Swarm robotics can be used for military applications such as surveillance, reconnaissance, search and rescue, target detection and neutralization, logistics support, and force protection. Swarm robots may also provide military personnel with greater situational awareness by monitoring large areas, detecting potential threats, and providing real-time data and enhancing the effectiveness and survivability of military operations by performing tasks that are too dangerous, difficult, or costly for humans or conventional systems (NATO n.d.2023). For instance, a swarm of robots could be used to search and rescue survivors in a disaster zone in order to conduct reconnaissance, gather intel or geo-mapping areas of interest, or identify potential threats or adversary positions. Swarm robots may also adapt to changing environments and scenarios by self-organizing, self-healing, and self-optimizing their behaviors.

Geo-Temporal Framework

The geo-temporal framework of military operations refers to the spatial and temporal aspects of warfighting, such as the geographic scope, scale, and distribution of forces and targets, the speed and duration of actions and effects, the synchronization and sequencing of operations, and the tempo and rhythm of warfare. The new technologies have the potential to expand, compress, distort, or transform this framework in unprecedented ways, creating new opportunities and challenges for military planners and decision-makers.

A geo-temporal framework is a method of analyzing and planning military action based on the spatial and temporal dimensions of the operational environment. It allows the commander to visualize the effects of different courses of action on the enemy, friendly forces, and the terrain, as well as the risks and opportunities involved. A geo-temporal framework consists of four elements: geospatial reference, temporal reference, geo-temporal analysis, and geo-temporal synchronization.

Geospatial reference is the process of defining and describing the physical features and boundaries of the area of operations. For example, a geospatial reference could include the coordinates, elevation, vegetation, roads, bridges, buildings, and other landmarks of a specific location. Geospatial reference helps the commander to understand the terrain and its impact on the operation.

Emerging disruptive technologies, such as artificial intelligence, drones, smart sensors, immersive technologies, and simulation, have the potential to impact the geospatial industry and transform how we collect, analyze, and visualize spatial data. Geospatial reference, or the process of assigning geographic coordinates to spatial features, is essential for integrating and harmonizing data from different sources and platforms, and for enabling spatial analysis and decision-making (NATO n.d.2022). However, geospatial reference also faces several challenges in the era of spatial big data, such as data quality, accuracy, interoperability, standardization, and privacy.

Artificial intelligence (AI), especially machine learning and deep learning, can enhance geospatial reference by automating the extraction of spatial features from various types of imagery and sensing data, such as satellite, aerial, drone, ground-based, and thermal images. AI can also improve the accuracy and efficiency of geo-referencing by learning from large amounts of labeled data and applying sophisticated algorithms to detect and correct errors, outliers, and inconsistencies. (Nato AI Strategy n.d. 2021). AI can also enable geospatial reference for dynamic and complex phenomena, such as human activities, environmental changes, and natural disasters, by incorporating temporal and contextual information.

Drones, or unmanned aerial vehicles (UAVs), can provide high-resolution and near-real-time imagery and sensing data for geospatial reference. Drones can capture data at different scales, angles, and perspectives, which can complement or supplement data from other platforms. Drones can also access remote or hazardous areas that are difficult or impossible to reach by humans or other vehicles (NATO n.d. 2022). Drones can also enable geospatial reference for moving objects or events by tracking their locations and trajectories.

Smart sensors and Internet of Things (IoT) devices can generate massive amounts of spatial data that can be used for geospatial reference. Smart sensors and IoT devices can measure various physical parameters, such as temperature, humidity, pressure, sound, light, motion, and vibration, and transmit them wirelessly to a central server or cloud platform. Smart sensors and IoT devices can also be embedded in objects or environments to monitor their status and performance (NATO n.d. 2022). Smart sensors and IoT devices can enable geospatial reference for fine-grained and continuous observations of spatial phenomena.

Immersive technologies, such as virtual reality (VR), augmented reality (AR), mixed reality (MR), and holograms, can create realistic and interactive representations of spatial data that can enhance geospatial reference. Immersive technologies can allow users to explore, manipulate, annotate, query, and experiment with spatial data in a three-dimensional (3D) environment. Immersive technologies can also overlay spatial data onto real-world locations using head-mounted displays or mobile devices, creating a seamless integration of physical and digital spaces (EARF n.d. 2023). Immersive technologies can enable geospatial reference for intuitive and engaging experiences of spatial phenomena.

Simulation technologies, such as agent-based modeling (ABM), cellular automata (CA), system dynamics (SD), and discrete event simulation (DES), can create synthetic spatial data that can be used for geospatial reference. Simulation technologies can model the behavior and interactions of spatial entities or agents based on rules or equations. Simulation technologies can also generate scenarios or outcomes based on different parameters or assumptions.

Simulation technologies can enable geospatial reference for testing hypotheses or evaluating policies related to spatial phenomena.

Temporal reference is the process of establishing and maintaining a common time system for all participants in the operation. Temporal reference ensures that everyone involved in the operation has a consistent and accurate understanding of when events occur and how long they last. Temporal reference also helps the commander to plan and execute the operation in a timely manner. One of the effects of emerging disruptive technologies is their impact on temporal reference, which is the way people perceive, organize, and use time in their activities. Temporal reference can affect various aspects of human behavior, such as decision-making, planning, motivation, but also well-being.

Geo-temporal analysis is the process of identifying and assessing the relevant factors and conditions that affect the operation, such as enemy capabilities, intentions, and vulnerabilities, friendly capabilities and limitations, weather, terrain, civil considerations, and time. Geo-temporal analysis helps the commander to determine the best course of action to achieve the objectives and desired effects.

The military geo-temporal analysis is using spatial and temporal data to understand the dynamics of conflicts, threats, and opportunities in different regions and scenarios. Emerging disruptive technologies, such as artificial intelligence, big data, cloud computing, and quantum computing, have the potential to transform this process by enabling faster, more accurate, and more comprehensive analysis of complex and uncertain situations (KPMG UK n.d. 2024). However, these technologies also pose significant challenges and risks for military geo-temporal analysis, such as ethical, legal, and social implications, data quality and security issues, adversarial manipulation and deception. Therefore, it is essential for military analysts and decision-makers to be aware of the benefits and limitations of these technologies, as well as the best practices and frameworks for their responsible and effective use.

Geo-temporal synchronization is the process of coordinating and integrating the actions of all elements of the joint force in time and space to achieve the desired effects. Geo-temporal synchronization ensures that all actions are aligned and harmonized to create a coherent and effective operation.

Military geo-temporal synchronization (MGTS) is the ability to coordinate the actions of different military units and assets across different geographic locations and time zones. MGTS is essential for achieving operational effectiveness, situational awareness, and joint interoperability. However, MGTS faces significant challenges from the emergence of disruptive technologies that may affect the accuracy, reliability, and security of geo-temporal information. Some of these technologies may include:

- Cyberattacks: may target the communication networks, data sources, and devices that enable MGTS, compromising their integrity and availability. For instance, cyberattacks can spoof, jam, or disrupt GPS signals, which are widely used for geo-temporal reference. Cyberattacks can also manipulate or destroy geo-temporal data stored in databases or transmitted over networks, causing confusion and misinformation among military decision-makers and operators (EARF n.d. 2023).

- Artificial intelligence (AI): may enhance the capabilities of MGTS by providing faster and more accurate analysis, prediction, and optimization of geo-temporal information. For example, AI can help identify optimal routes, schedules, and targets for military operations based on geo-temporal constraints and objectives. AI can also help detect and mitigate cyberattacks on MGTS by monitoring and responding to anomalies and threats. However, AI can also pose risks to MGTS by creating new vulnerabilities and uncertainties. Thus, AI has the ability to generate realistic but fake geo-temporal information that can deceive or mislead human users. AI can also behave unpredictably or autonomously, violating ethical or legal norms or conflicting with human intentions (Nato AI Strategy n.d. 2021).

- Quantum technologies: are offering new possibilities and advantages for MGTS by exploiting the unique properties of quantum physics. For example, quantum technologies can enable more precise and secure geo-temporal measurements and communications using quantum sensors, clocks, and encryption. Quantum technologies can also enable faster and more complex geo-temporal computations using quantum computers (DoD’s n.d. 2021) However, quantum technologies can also challenge MGTS by introducing new complexities and uncertainties. For instance, quantum technologies can create new sources of error and noise that can affect the accuracy and reliability of geo-temporal information. Quantum technologies can also create new asymmetries and threats that can undermine the security and stability of MGTS.

These emerging disruptive technologies have profound implications for MGTS, requiring new strategies, policies, and standards to adapt to the changing geo-temporal environment. Military leaders and planners need to be aware of the opportunities and challenges posed by these technologies, and leverage them to enhance MGTS while mitigating their risks.

Conclusions

Emerging disruptive technologies can provide opportunities for the development of society and security, but also pose challenges and risks, such as changing the physiognomy of armed conflict, creating new security architectures, and modifying international relations. They may increase the role of strategic deterrence and reduce the need for effective defense, which can be beneficial for preventing wars and saving lives.

They can help militaries become more effective, resilient, cost-efficient, and sustainable. NATO and its Allies may find emerging disruptive technologies useful for maintaining their technological edge, fostering innovation, and establishing principles of responsible use, but also as a requirement for adapting and transforming their security systems and cooperation with other international organizations.

Disruptive technologies may offer militaries an advantage and deterrent value, but also create new vulnerabilities and dependencies, as well as increase the complexity and uncertainty of the operational environment. They may alter the character of conflict and become key arenas of global competition, raising ethical challenges regarding the acquisition and use of force, and may create technological gaps and dependencies among allies and partners.

BIBLIOGRAPHY:

1. DoD's. 2021. China Military Power Report: How Advances in AI and Emerging Technologies Will Shape Competitiveness - Council on Foreign Relations.
2. EARF.(Euro-Atlantic Resilience Forum).n.d. Accessed Ianuary 20, 2024. https://resilienceforum.e-arc.ro/wp-content/uploads/2023/12/EARF2023-Conclusions-EDT.pdf
3. NATO's new AI strategy. n.d. 2021. Accessed Ianuary 20, 2024. https://natowatch.org/sites/default/files/2021-11/briefing_88_nato_ai_strategy.pdf.
4. NATO. 2023. NATO - News: New focus on emerging and disruptive technologies helps NATO stay ahead of the curve. n.d. Accessed Ianuary 20, 2024. https://www.nato.int/cps/en/natohq/news_181901.htm.
5. NATO. 2022. NATO - Topic: Emerging and disruptive technologies. n.d. Accessed Ianuary 20, 2024. https://www.nato.int/cps/en/natohq/topics_184303.htm.
6. Parlamentul European. “Raport referitor la tehnologiile critice pentru securitate și apărare: situația actuală și provocările viitoare”. n.d. Accessed Ianuary 16, 2024. https://www.europarl.europa.eu/doceo/document/A-9-2023-0120_RO.html

7. Stanciu, Cristian-Octavian. Gimiga, Silviu-Iulian. 2023. New technologies and their impact in the military field, “Buletinul UNAp”, Nr.2/2023, https://buletinul.unap.ro.
8. US- Defense Primer: Emerging Technologies. n.d. Accessed Ianuary 30, 2024. https://crsreports.congress.gov/product/pdf/IF/IF11105
9. US- Critical and Emerging Technologies List Update - The White House. n.d. Accessed Ianuary 20, 2024. https://crsreports.congress.gov/product/pdf/IF/IF11105. https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf
10. UK- National AI Strategy - GOV.UK. n.d. Accessed Ianuary 20, 2024. https://www.gov.uk/government/publications/national-ai-strategy.
11. UK- Emerging and disruptive technologies - KPMG United Kingdom. n.d. Accessed Ianuary 17, 2024. https://kpmg.com/uk/en/home/misc/board-leadership-centre/emerging-and-disruptive-technology.html.
12. Zak, Dychtwald. 2021. “China’s New Innovation Advantage”. Harvard Business Review. Accessed Ianuary 20, 2024. https://hbr.org/2021/05/chinas-new-innovation-advantage.

1053477-3045-1396-24-06

CHALLENGES WITHIN THE NEW NATIONAL AND EURO-ATLANTIC RESILIENCE CONTEXT

Titus-Vlad GALANTON
Master students, „Carol I" National Defence University, Bucharest, Romania
E-mail: titus_galanton@yahoo.com

Florin-Vasile RADU
Master students, „Carol I" National Defence University, Bucharest, Romania
E-mail: radu.vasile5@yahoo.com

Abstract: *In an era characterized by contested geopolitical landscapes and the emergence of diverse threats, the resilience of states in the face of these challenges requires increasingly complex analysis. At the heart of the analysis is the role of NATO and its strategic evolution in response to these threats generated by new technologies that also require innovative strategies. In this context, current strategies used by national and Euro-Atlantic entities to enhance military resilience will be assessed. Thus, new threats require new international collaborations, as can be seen in the ongoing Russian-Ukrainian conflict. In this context, reference will also be made to a shift in the paradigm of military strategy after the Cold War, highlighting the imperative of resilience in the face of contemporary challenges. The aim of the article is to provide a comprehensive understanding of the need to implement collective and proactive defense mechanisms and policies that can effectively overcome the obstacles posed by the geopolitical arena of the 21st century.*

Keywords: *paradigm, resilience, emerging technologies, anti-satellite warfare, cyber warfare*

Introduction

In the intricate tapestry of global security, the Euro-Atlantic region stands as a pivotal area where the threads of national and collective defense are continuously tested and redefined. The post-Cold War era has witnessed a significant transformation in military threats and challenges, necessitating a paradigm shift in defense strategies. This shift is not merely a response to conventional military threats but also an adaptation to the complexities of modern warfare, including cyber threats, hybrid warfare, and the resurgence of great power competitions.

At the heart of this discourse is the concept of resilience – the ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions. In the military context, resilience has transcended beyond mere survival or passive endurance; it has become a proactive strategy, an integral part of national security policies and international defense collaborations. This notion of resilience is particularly pertinent in the Euro-Atlantic region, where diverse member states grapple with the challenges of maintaining security and stability amidst a landscape rife with both traditional and non-traditional threats. In contemporary security parlance, resilience represents more than enduring hardships; it encapsulates the capacity to adapt and evolve in the face of diverse threats.

The Euro-Atlantic region's strategic importance cannot be overstated. It is not just a geographical expression but a symbol of a complex security ecosystem that involves key players like NATO, the European Union, and various national governments. These entities are continuously adapting their policies and strategies to address the multifaceted nature of threats that characterize the 21st century. Reflecting on this, the Euro-Atlantic region's security landscape reflects global trends, where cyber warfare and conventional military threats coexist and interplay.

Through this paper, we aim to delve into the nuances of these challenges, exploring how the Euro-Atlantic region, with its rich history and complex present, is navigating the path of resilience. We will analyze the transformation of defense strategies, the role of international alliances, and the impact of technological advancements in shaping the future of military defense. In doing so, the paper contributes to a deeper understanding of the intricate balance between maintaining robust defense postures and fostering an environment of peace and stability in an increasingly unpredictable global order.

1. Historic Context

The Euro-Atlantic area has been central to global security dynamics since the end of World War II. This region, primarily encompassing Europe and North America, has experienced significant shifts in security policies and alliances, most notably through the establishment and evolution of the North Atlantic Treaty Organization (NATO). Following World War II, the Euro-Atlantic security landscape was shaped by the emergence of the Cold War, a period of geopolitical tension between the Soviet Union and Western powers. In 1949, NATO was formed as a collective defense alliance to counter Soviet expansion in Europe. The early years of NATO focused on deterrence, military readiness, and the principle of collective defense, as articulated in Article 5 of the NATO Treaty.

The Cold War era was marked by a stark division of Europe into Eastern and Western blocs, with NATO and the Warsaw Pact as the respective military alliances. This period saw the establishment of a nuclear deterrent strategy, the balance of power politics, and a series of crises that brought the world to the brink of nuclear war, such as the Cuban Missile Crisis. The dissolution of the Soviet Union in 1991 marked a significant turning point for Euro-Atlantic security. The end of the Cold War led to a reevaluation of security policies and the role of NATO. The alliance underwent a process of transformation, embracing new missions and expanding its membership eastward to include former Warsaw Pact countries and parts of the former Soviet Union through the Partnership for Peace program. This era also saw NATO engaging in peacekeeping and crisis management operations in the Balkans, demonstrating a broader security mandate beyond collective defense against a state adversary.

The September 11, 2001, terrorist attacks on the United States marked another pivotal moment for Euro-Atlantic security, shifting the focus towards non-state actors and transnational threats. NATO invoked Article 5 for the first time in its history, signaling a collective response to terrorism. The alliance's subsequent involvement in Afghanistan represented a significant operational shift, focusing on counter-terrorism, nation-building, and counter-insurgency. This period underscored the need for NATO to adapt to new security challenges, including terrorism, piracy, and the proliferation of weapons of mass destruction.

Today, the Euro-Atlantic security environment faces a complex array of challenges. Russian assertiveness, as evidenced by the annexation of Crimea and involvement in Eastern Ukraine, has reignited concerns over territorial integrity and sovereignty in Europe.

The turning point in the modern understanding of the Russian threat came with the 2008 war in Georgia, which served as a stark reminder of Russia's willingness to use military force to achieve its geopolitical objectives. This conflict was a precursor to the more significant and still-unresolved crisis in Ukraine, beginning with the annexation of Crimea in 2014 and the subsequent support for separatist movements in Eastern Ukraine. These actions not only violated international law and the sovereignty of Ukraine but also shattered any remaining illusions of a post-Cold War era characterized by cooperative security arrangements between Russia and the West. Russia's military actions have been accompanied by a sophisticated strategy of hybrid warfare, blending conventional military force with cyber-attacks, disinformation campaigns, and the leveraging of economic power to influence political outcomes within Euro-Atlantic countries. The use of cyber warfare has been particularly concerning, with attacks targeting critical infrastructure, electoral processes, and the dissemination of fake news to sow discord and undermine trust in democratic institutions. These tactics represent a deliberate attempt to exploit the vulnerabilities of open societies and to challenge the post-World War II international order. However, military preparedness is only one aspect of addressing the Russian threat. There is also a critical need for strengthening cyber defenses, enhancing the resilience of critical infrastructure, and combating disinformation. Equally important is the need for a coherent strategy that addresses the vulnerabilities associated with energy dependence and seeks to diversify energy sources.

The Euro-Atlantic community must also engage with other global powers and regional actors to build a broad-based coalition that can present a united front against attempts to undermine international norms and institutions. This includes working closely with partners in Asia, the Middle East, and Africa to counterbalance Russia's efforts to expand its influence and to promote a rules-based international order.

The evolution of Euro-Atlantic security reflects the changing dynamics of global politics and the persistent need to address both conventional and unconventional threats. As the world enters a new era of strategic competition, the ability of the Euro-Atlantic community to adapt and respond to emerging challenges will be crucial in maintaining peace and stability in the region.

2. Contemporary Challenges

The contemporary security landscape of the Euro-Atlantic region is marked by a diverse array of challenges that extend beyond conventional military threats. This multifaceted environment is characterized by the emergence of cyber warfare, hybrid threats, and a re-escalation of traditional state-based conflicts.

2.1. Cyber Warfare and Hybrid Threats

The digital age has brought forth the specter of cyber warfare, with state and non-state actors capable of orchestrating attacks on critical infrastructure and information systems. Cyber warfare represents a paradigm shift in military strategy, where invisible cyber-attacks can have tangible, destructive consequences. These threats are not confined to the digital realm but often manifest in hybrid forms, combining cyber tactics with conventional and unconventional methods. Hybrid warfare blurs the lines between traditional conflict and subversive tactics, posing a unique challenge to Euro-Atlantic security.

Cyber warfare and hybrid threats represent some of the most sophisticated and insidious challenges within the new national and Euro-Atlantic resilience context. These threats are characterized by their multifaceted nature, blending conventional military power with cyberattacks, disinformation campaigns, and other non-traditional tactics. Addressing these threats requires an in-depth understanding of their implications and the formulation of comprehensive strategies to bolster resilience.

Cyber warfare involves the use of digital attacks by state or non-state actors to disrupt, damage, or destroy the critical infrastructure of a nation or to infiltrate and steal information. This form of warfare has become a tool of choice for many actors due to its low cost, deniability, and the potential for significant impact. The key challenges in the cyber domain include infrastructure vulnerability, sophistication of attacks and information operations.

Critical national infrastructure, including power grids, financial systems, and healthcare services, is increasingly interconnected and dependent on digital technologies. This interconnectivity, while beneficial for efficiency and functionality, also presents vulnerabilities that adversaries can exploit to cause widespread disruption.

The techniques used in cyber warfare are becoming more sophisticated, including advanced persistent threats (APTs), ransomware, and state-sponsored hacking. These sophisticated attacks can bypass traditional cybersecurity measures, making detection and defense more challenging.

Beyond targeting physical infrastructure, adversaries use cyber operations to manipulate information, spread disinformation, and undermine trust in institutions. These operations aim to influence public opinion, sow discord, and destabilize societies from within.

Hybrid threats combine military and non-military tactics, cyber operations, and disinformation to achieve strategic objectives without escalating to open warfare. These threats are designed to exploit the gray zone between peace and war, making it difficult for targeted nations and alliances to respond effectively.

Hybrid warfare strategies often involve ambiguous actions that complicate attribution and response. The use of proxy forces, cyber mercenaries, and covert operations creates plausible deniability, hindering effective countermeasures.

Adversaries engaging in hybrid warfare exploit gaps in international law and norms, operating in spaces that are not clearly regulated. This allows them to undermine national and international security without triggering a conventional military response.

Hybrid threats are designed to have a psychological impact, undermining confidence in government institutions and destabilizing societies. The use of propaganda, disinformation, and cyberattacks on civilian targets aims to erode trust and cohesion within and among nations.

Addressing the challenges posed by cyber warfare and hybrid threats requires a multifaceted approach that enhances resilience at national and Euro-Atlantic levels. Nations and alliances must invest in advanced cybersecurity technologies, develop cyber defense doctrines, and enhance the cybersecurity literacy of their populations. Public-private partnerships are essential for protecting critical infrastructure and sharing threat intelligence.

Countering disinformation and propaganda requires efforts to promote media literacy, support independent journalism, and develop capabilities to rapidly identify and counter false narratives.

The international community must work together to close the gaps in international law and norms that hybrid threats exploit. This includes developing consensus on the applicability of international law in cyberspace and norms for state behavior.

Unity and cooperation among nations and within alliances are crucial for effectively countering hybrid threats. This involves sharing intelligence, coordinating responses to incidents, and supporting nations that are targets of cyberattacks and hybrid warfare tactics.

2.2. Resurgence of Conventional Military Threats

Recent years have seen a resurgence of traditional military tensions in the Euro-Atlantic region, particularly along its Eastern borders. The conflict in Ukraine and the growing assertiveness of Russia have renewed focus on collective defense and deterrence strategies within NATO. The Euro-Atlantic region is witnessing a return to conventional military posturing, reminiscent of the Cold War era, but underpinned by 21st-century geopolitical realities.

The post-Cold War era saw a temporary decrease in the focus on conventional military threats as international attention shifted towards non-state actors and asymmetric warfare (e.g., terrorism, cyber-attacks). However, recent years have witnessed a return of state-centric tensions, notably with the rise of China, the assertiveness of Russia in Eastern Europe and the Middle East, and ongoing disputes in regions such as the South China Sea. These rivalries necessitate a renewed focus on conventional military capabilities.

Countries across the Euro-Atlantic area and beyond are modernizing their armed forces, investing in new technologies, and increasing their military budgets. This modernization includes the procurement of advanced aircraft, naval vessels, and land systems, as well as investments in cyber capabilities and space defense, reflecting a comprehensive approach to national and alliance defense strategies.

In response to the evolving security environment, NATO has taken steps to enhance its deterrence and defense posture. This includes increasing the readiness of its forces, enhancing forward presence in Eastern Europe, and adapting its command structure to better address hybrid and cyber threats alongside conventional challenges.

The resurgence of conventional threats tests the credibility of collective defense mechanisms. Ensuring the effectiveness of deterrence strategies in the Euro-Atlantic area involves not only military preparedness but also political will and unity among alliance members. The challenge is to maintain a balance between deterring aggression and avoiding escalation in tensions.

Resilience against conventional military threats requires a holistic approach that encompasses not only military readiness but also economic stability, societal cohesion, and robust critical infrastructure. The concept of resilience has expanded to include the ability to withstand and quickly recover from direct military aggression.

The integration of emerging technologies such as artificial intelligence (AI), unmanned systems, and hypersonic weapons into military doctrines is transforming the nature of conventional threats and defense capabilities. These technologies offer both opportunities for enhanced defense mechanisms and challenges in terms of arms control and maintaining strategic stability.

The resurgence of conventional military threats underscores the importance of international arms control and disarmament efforts to prevent an arms race and reduce the risk of conflict. This includes not only traditional arms control treaties but also new agreements that address emerging technologies and domains of warfare.

2.3. The Role of NATO

In response to these diverse challenges, NATO has been pivotal in coordinating a collective response, adapting its strategies to meet both conventional and unconventional threats. The Alliance's 2020 Strategic Concept reflects this adaptive approach, emphasizing the need for a comprehensive defense strategy. NATO's evolving strategic concept is a testament to the Alliance's commitment to addressing the full spectrum of threats in the Euro-Atlantic region.

NATO remains committed to its core function of collective defense, as enshrined in Article 5 of the North Atlantic Treaty. The Alliance has responded to the resurgence of conventional military threats from state actors by enhancing its military readiness and capabilities. This includes increasing the presence of NATO forces in Eastern Europe, conducting regular military exercises, and developing rapid response forces to ensure a credible deterrent posture against potential aggression.

Recognizing the growing significance of cyber threats and hybrid warfare tactics, NATO has prioritized enhancing the cyber defenses of member states and improving resilience against disinformation, election interference, and other forms of hybrid attacks. The establishment of the Cyberspace Operations Centre and the recognition of cyberspace as a domain of operations are key milestones in this area.

NATO has adapted its strategies to contribute to international counterterrorism efforts. This includes intelligence-sharing, capacity-building initiatives in partner countries, and direct involvement in missions and operations designed to combat terrorism and stabilize conflict regions, such as the NATO mission in Afghanistan (ended in August 2021).

The Alliance is also focusing on understanding and integrating emerging technologies, such as artificial intelligence (AI), quantum computing, and biotechnology, which have significant implications for defense and security. NATO aims to maintain a technological edge while also considering the ethical and legal implications of these technologies.

A key aspect of NATO's role in the contemporary security environment is its focus on resilience. This includes ensuring that member states have robust civil preparedness, supply chain security, and infrastructure resilience to withstand and quickly recover from a wide range of threats, including military attacks, natural disasters, and pandemics.

These contemporary challenges underscore the complexity of maintaining security and resilience in the Euro-Atlantic region. The dynamic nature of these threats necessitates a flexible and multifaceted approach to defense, leveraging both traditional military capabilities and innovative technologies.

3. Case Study

The contemporary security challenges of the Euro-Atlantic region are best understood through specific case studies that highlight the complex nature of modern threats and the responses they require. The Russian-Ukrainian conflict is a case in point.

This conflict exemplifies the re-emergence of conventional military threats in the Euro-Atlantic region, but also the increasing interest in the space environment, inaccessible to conflict as defined by existing international law. With this conflict, new horizons have opened up that mankind did not think possible a few years ago. The Russian-Ukrainian war has significant implications for regional stability and NATO's strategic calculus. This conflict is not just a regional problem, but a decisive test of the integrity and resilience of the Euro-Atlantic security architecture. The conflict underlines the need for a robust collective defense mechanism and the challenges of responding to territorial aggression in the 21st century.

3.1. The dawn of a new conflict horizon

At the end of 2022, Konstantin Vorontsov, head of the non-proliferation and arms control department of the Russian Ministry of Foreign Affairs, addressed the first committee of the United Nations General Assembly. He highlighted a worrying trend evident during recent events in Ukraine, highlighting the use by the United States and its allies of civilian infrastructure in outer space for military purposes, which extends beyond benign technological uses. Vorontsov warned that such infrastructure could become viable targets for retaliation, marking a significant departure from past practices when states refrained from formally considering destroying adversaries' space assets. This statement attracted widespread attention, appearing prominently in Western newspapers alongside discussions of possible Russian actions against commercial satellites. Particularly commercial constellations had previously been considered off-limits for orbital attack due to their perceived lack of military relevance.

The conflict in Ukraine, while not the first inaugural space war, witnesses a systematic integration of outer space into military operations, including activities carried out by private entities in a military context, such as jamming and orbital challenges. This conflict highlights a new dynamic in the role of outer space in high-intensity warfare. Even before the Ukrainian crisis, space emerged as a strategically advantageous area, prompting various powers to invest in its exploration and exploitation for military purposes. After 24 February 2022, space became an active theatre of conflict as two space coalitions gradually positioned themselves against each other. Consequently, the conflict requires an examination of contemporary and future modes of space warfare, moving from a previously uncontested domain to a potential arena of confrontation.

The involvement of outer space in military operations predates the Ukrainian conflict, with many scholars and military analysts pointing to the Gulf War as the first significant 'space conflict'. In this conflict, space assets, primarily satellites, played a key role in operational needs, particularly in terms of intelligence gathering and targeting. Since then, the use of these assets has expanded, and the war in Ukraine is no exception, as each side involved relies on space assets to enhance combat capabilities.

In recent years, outer space has been constantly exploited as a distinct theatre of operations. The armed forces of different countries are reallocating resources to space-related efforts, but such efforts require substantial budgets and are not universally prioritized. Some nations are moving towards harnessing the capabilities of their allies or, increasingly, private companies. The substantial increase in investment over the past decade has shaken up the sector, as demonstrated by the deployment of private satellite constellations such as SpaceX's Starlink. National programs alone are struggling to meet the growing demand for access to these next-generation technologies. For countries without their own space assets, private companies provide a lifeline, offering support when needed, as seen in Ukraine at the start of the conflict.

The use of space assets in military operations is increasing, requiring protection against both natural hazards and malicious actions. While Western space powers perceived the destruction of a non-functional Russian satellite by a Nudol rocket in October 2021 as a provocation, various other threats are looming in the space environment. Even seemingly isolated actions in orbit can lead to damage, such as spy satellites approaching adversaries' military satellites, direct deployment of objects in orbit, attempts to approach or eavesdrop, and jamming of signals. Russia possesses most of these offensive capabilities in space and routinely tests them, presenting their evidence to other space actors, especially during a period of challenge in its space program.

The conflict in Ukraine did not start with a grandiose anti-satellite operation, the spectacular destruction of enemy satellites or the widespread jamming of Ukrainian and NATO assets in the region. However, it would be a mistake not to consider the space environment from the early stages of the conflict, as the war in Ukraine effectively began in space with a cyber-attack in February 2022 on the Viasat satellite network and KA-SAT terminals. Given the absence of Ukraine's national space assets and Russia's initial reluctance to directly challenge NATO, there was no significant disruption to the space environment at the start of the conflict. This approach aligned with Russian rhetoric, stressing that this was an operation rather than a full-scale war. However, Moscow's evolving position, which increasingly refers to direct confrontation with the US or NATO in the Ukrainian theatre, gives weight to the possibility of Russian aggression in space.

3.2. Repeated appearances in space competition

In 2022, there were a significant number of Russian military launches into space, involving the deployment of 14 satellites. In August of the same year, Russia launched a military satellite, Kosmos-2558, into low orbit near the US intelligence satellite, USA-326. Identified as a Nivelir inspector satellite, sharing the design of its predecessors 2519 and 2542 launched in 2017 and 2019, it potentially possesses orbital projection capability, as noted by Bart Hendrickx, a Russian space expert. Any provocative action near the US intelligence satellite USA-346 could have substantial strategic and diplomatic implications. In other news, a year later (January 2023), the 2499 satellite, a mysterious military inspector launched in 2014 suspected of having anti-satellite capabilities, underwent an orbital "decay", according to the US Space Forces 18th Space Defense Squadron. This event generated space debris, leading to speculative media chatter that alluded to a potential demonstration of Russian space kamikaze actions.

Shifting the focus to a more distant horizon, two months later (March 2023), a military electromagnetic intelligence and communications satellite called Luch-Olymp was launched, like its 2018 predecessor involved in listening operations of the French-Italian geostationary military communications satellite AthenaFidus. Although most of Russia's operations in space take place in low orbits, it has recently expanded its interest to higher and more distant orbits. Russia's offensive actions in space serve as a pointer to larger offensives, aimed at providing time for training and partial occupation of space. Despite not having total superiority, Russia, along with the United States and China, hosts dedicated programs in this area.

Russian aerospace forces, facing constraints of a capability greater than available resources, refrain from engaging in open space warfare. Instead, Russia adopts intermittent maneuvers as guerrilla tactics for training, destabilizing adversaries, impressing, and occasionally disrupting specific equipment. This asymmetric and covert military response aligns with the evolving landscape of space warfare.

An article written by three Russian Armed Forces research officers in March 2023 argues that the space warfare theatre encompasses exo-atmospheric space, hosting orbital constellations of space systems with dual-use capabilities. This deployment, either in space or on Earth, is seen as the precursor to the next revolution in the military. Today, space manifests two battlefronts: one crucial for essential integrated battlefield support, requiring operational agility, and another focus on combat, which began well before 24 February 2022. This multi-domain approach reflects the emerging military dimension of space, incorporating a dual-use arsenal.

4. Strategies for Resilience

The current security environment in the Euro-Atlantic region demands a multifaceted approach to resilience, incorporating both traditional and innovative strategies. The key strategies that are used to strengthen military and security resilience in the face of contemporary challenges are:

International Cooperation and Intelligence Sharing: The complexity of modern security threats necessitates enhanced cooperation among Euro-Atlantic nations and beyond. Effective intelligence sharing has become crucial in preempting and responding to threats. We can say that in an era of interconnected threats, the strength of the Euro-Atlantic security lies in the collective and cooperative approach to intelligence sharing and strategic planning. This collaboration extends to sharing best practices, technologies, and coordinated responses to crises.

Intelligence sharing played a crucial role in the context of the Ukraine war. Weeks before the actual Russian invasion occurred, the US intelligence community had gathered information about the impending action and disclosed this to the media. This early insight facilitated swift coordination with Western allies and provided substantial support to the Ukraine's secret service in the early stages of the conflict. Achieving these objectives would not have been possible without a strong collaboration between global intelligence services, encompassing contributions from the private sector as well. This partnership underscores the essential nature of international intelligence cooperation in navigating and responding to modern geopolitical challenges.

Innovative Defense Technologies: The rapid advancement of technology offers new avenues for enhancing defense capabilities. The integration of artificial intelligence, unmanned systems, and advanced surveillance technologies are reshaping military strategies. The adoption of AI and unmanned systems in military operations is not just an enhancement of capabilities but a fundamental shift in warfare.

The strategic implications of these technologies are profound. They offer the potential for increased effectiveness and efficiency in operations, enhanced force protection, and the ability to project power in new and innovative ways. However, they also raise important questions regarding the rules of engagement, the control of autonomous systems, and the prevention of escalation in conflicts driven by rapid, AI-enabled decisions.

Cybersecurity Measures: In response to the growing threat of cyber warfare, Euro-Atlantic nations are prioritizing the strengthening of their cybersecurity infrastructure. Initiatives include developing robust cyber defense mechanisms, conducting regular cyber exercises, and fostering public-private partnerships in cyber defense. NATO and the EU share information between cyber response teams and exchange best practices. Cooperation is also being enhanced in areas including training, research, and exercises, with tangible results in countering cyber threats. Building resilient cybersecurity infrastructure is as crucial as physical defenses in the current landscape of hybrid warfare.

In this tumultuous period, military entities must brace for formidable challenges by forging a robust and cyber-resilient command infrastructure. This necessitates the harmonization and seamless integration of planning activities alongside electronic warfare command. Given the evolution of warfare from traditional to non-traditional forms, and from symmetric conflicts to asymmetric and hybrid engagements, it is imperative that cyber operations are strategically crafted. These operations should not only aim to protect but also to ensure the enduring functionality of military assets.

Adaptability and Continuous Training: The unpredictable nature of modern threats requires military and security forces to be highly adaptable and continuously trained in new tactics and technologies. Regular training exercises, simulations, and the adoption of flexible operational doctrines are key to maintaining a state of readiness. The agility and adaptability of the armed forces in responding to unconventional threats are as vital as their combat capabilities. "Research to date suggests that the task of developing an adaptability training strategy should serve as the forerunner of the larger task of creating an overall strategy for developing more adaptable individuals and institutions throughout the military" (Freeman and Burns 2010, 12).

These strategies collectively contribute to the resilience of the Euro-Atlantic region's military and security apparatus, highlighting the need for a dynamic, proactive approach to defense in the face of evolving global challenges.

5. Future Outlooks

Emerging Threats and Evolving Strategies: The trajectory of military threats is undergoing a profound transformation, propelled by the advent of emerging technologies such as cyber-physical systems and artificial intelligence. These technologies are not only redefining the battlefield but also the nature of the threats themselves. The integration of these emerging technologies is set to play a decisive role in shaping the future of Euro-Atlantic security. The challenge lies in not just understanding these technologies but integrating them into military doctrines in a manner that enhances defense capabilities while mitigating vulnerabilities.

Anticipating Technological Shifts: The ability to anticipate and prepare for the impact of technological advancements on security dynamics is crucial. This requires continuous investment in research and development (R&D), as well as fostering innovation within military and defense frameworks.

Adapting Military Doctrines: The adaptation of military strategies to include cyber and AI capabilities is essential for maintaining strategic advantages. This involves training personnel, developing new operational doctrines, and ensuring ethical considerations are integrated into AI deployment in military operations.

Strengthening Alliances and Partnerships: The significance of international alliances, especially NATO, is poised to escalate in the face of collective security challenges. The robustness of these alliances and the capability to orchestrate cohesive responses are fundamental to the future security of the Euro-Atlantic region. Enhancing these partnerships and exploring new alliances are strategic imperatives.

Enhancing NATO's Role: Strengthening NATO's operational capabilities and ensuring its readiness to confront hybrid threats, including cyber-attacks and misinformation campaigns, are pivotal.

Fostering New Partnerships: Beyond traditional alliances, there is a need to cultivate partnerships with non-NATO countries, international organizations, and even private entities, especially in the realms of cybersecurity and technological innovation.

Economic Resilience: Strengthening economic foundations and ensuring energy security are crucial for reducing vulnerability to external shocks and pressures.

Environmental Security: Addressing climate change and its security implications is vital for preventing resource conflicts and ensuring long-term regional stability.

Conclusions

The Euro-Atlantic region stands at a critical juncture in its security history, facing an increasingly complex and multifaceted array of challenges. From the persistent shadow of state-based confrontations to the nebulous realms of cyber and hybrid warfare, the spectrum of threats has broadened and intensified. This analysis aims to underscore the importance of adaptability, innovation, and collective action in navigating these challenges, laying the groundwork for a resilient security posture in the Euro-Atlantic area.

Recent history, marked by events such as the Russian-Ukrainian conflict and sophisticated cyber-attacks on critical infrastructure, serves as a stark reminder of the dynamic nature of contemporary threats. These case studies not only illustrate the varied facets of modern warfare but also highlight the critical need for an adaptive and forward-looking defense strategy.

The complexity of the current security environment demands a departure from traditional defense paradigms. The incorporation of innovative technologies, the enhancement of cyber resilience, and the strengthening of collective defense mechanisms emerge as pivotal elements in this transformative journey. It's not just about responding to threats as they arise but about anticipating and neutralizing them through strategic foresight and preparedness.

The role of NATO and other international alliances has never been more crucial. In the face of escalating security challenges, these alliances represent the collective resolve to defend peace and stability in the Euro-Atlantic region. The efficacy of such partnerships, however, hinges on their ability to foster unity, share intelligence, and coordinate strategic responses to emerging threats.

To navigate the uncertain waters of the future security landscape, the Euro-Atlantic region must embrace a comprehensive approach that encompasses not only military capabilities but also diplomatic, technological, and societal dimensions.

The strategic integration of advanced technologies into military and security frameworks offers a critical lever for enhancing operational capabilities. From AI-driven threat detection to blockchain for secure communications, the potential of technology to revolutionize defense strategies is immense. However, this technological pivot must be balanced with ethical considerations and safeguards against new vulnerabilities.

A holistic understanding of security, which includes economic stability, environmental sustainability, and social cohesion, is essential for addressing the root causes of conflict and building long-term resilience. This approach recognizes that the strength of a region's security is as much about the robustness of its societies and economies as it is about its military capabilities.

The path to a secure and stable Euro-Atlantic region is one of continuous adaptation, innovation, and collective effort. By embracing a multifaceted strategy that integrates advanced technologies, strengthens alliances, and adopts a comprehensive view of security, the region can effectively navigate the challenges of today and tomorrow. The future of Euro-Atlantic resilience, therefore, lies in the unwavering commitment to collaborative defense and the proactive pursuit of a peaceful, secure, and prosperous region for generations to come.

BIBLIOGRAPHY:

1. Biddle, S. & Friedman, J. A. 2019. The New Context for Military Resilience: Adaptation and Innovation in a Changing World. Oxford University Press.
2. Freeman, W.D, Burns, W. R. Jr. Developing an Adaptability Training Strategy. https://www.ida.org/-/media/feature/publications/d/de/developinganadaptabilitytrainingstrategy/developinganadaptabilitytrainingstrategy.ashx.
3. Greene, T. & Oliker, O. 2023. The New Cold War: Euro-Atlantic Tensions in the 21st Century. Princeton University Press.
4. Karaman, M., Çatalkaya, H. & Aybar C. 2016. Institutional Cybersecurity from Military Perspective, International journal of information security science, vol 5, nr. 1.
5. Klimburg, A. 2012. National Cyber Security Framework Manual. NATO CCD COE Publications.
6. Kovalev, A.P., Sotnik, S.A., Sotnik, D.S. 2023. Space as a new sphere of armed struggl*e*. https://vm.ric.mil.ru/upload/site178/lCmCpEOiWw.pdf.
7. Krinitsky, Y. 2022. Considerations for the development of ways and methods of action for aerospace defence forces. Voennaya Mysl. (https://vm.ric.mil.ru/Stati/item/388551/).
8. Peterson, L. 2021. Hybrid Warfare and Euro-Atlantic Security. Yale University Press.
9. Smith, R. 2021. Euro-Atlantic Security in the 21st Century: A New Era of Challenge and Response. Cambridge University Press.
10. US Civilian Space Facilities in Ukraine May come Under Retaliatory Attack—Russian News Agency. TASS. 16 February 2023. (https://tass.com/defense/1577235).
11. Wagner, S. 2022. Cyber Warfare in the 21st Century. MIT Press.
12. ***Cyberspace Operations. Joint Publication (JP) 3-12. 2018.
13. ***https://www.australiandefence.com.au/news/sponsored/ai-the-game-changer-in-modern-warfare.

1053477-3045-1396-24-07

NORTH ATLANTIC ALLIANCE AND THE DYNAMICS OF POWER BALANCE

Petru Marius SABOU
Counselor to the Chamber of Deputies, Parliament of Romania, Bucharest, Romania
E-mail: petrumariussabou@gmail.com

***Abstract**: The balance of power is considered to be a self-help mechanism, support, and cooperation in an anarchic international system, specifically one in which there are no supranational structures to impose specific behaviors or decisions on states. Both balancing and alignment are considered attributes of the balance of power, and balancing against the Soviet Union ultimately led to the formation of the North Atlantic Alliance. Thus, after the end of the Cold War, the same process helped in the reconfiguration and adaptability of the Alliance. The reconfiguration of political and national values in relation to power interests is considered a permanent process at the state level. From this perspective, it is of interest how states configure both their cooperation with other states and the development of their own military capabilities.*

***Keywords**: supranational structures, anarchy, balance of power, military capabilities, cooperation.*

Introduction

During the Cold War, the *balance of power* was ensured by the two major power *poles* of the Second World War, namely the USA and the USSR. However, the formation of the North Atlantic Alliance was subsequently seen as an instrument aimed at protecting Western European states. Nevertheless, this is not a unique perspective, and *analyzing the formation of NATO from a realist* standpoint can provide a more comprehensive view. Realists believe that states form alliances to ensure their own security. At the beginning of the Cold War, although invested with confidence by Western chancelleries, the Alliance was rather seen as having greater political than military significance. (Constantinescu Mihnea, in Eugen Preda's "NATO-A Brief History," published by Cultural Foundation Magazine Historia, Bucharest 1999, p.5.)

It is very possible, however, that military strategies may have had underlying political actions at the domestic level, as essential conditions for creation. Edward Kolodziej argues that all security-related aspects are essentially political issues. Thus, aiming to ensure security, NATO also raises a political issue.

The formation of the Alliance had two major objectives: protecting the West from Soviet and communist expansion, and at the same time, from any other kind of dangers. However, the existence of the strategic threat imposed the subordination of the other purposes.

In this way, the acceptance into the Alliance of states that could hardly be considered truly democratic can be explained. (Fidler Jiri, Petr Mares, "History of NATO," published by European Institute, Iaşi, 2005, p.7.) With the aim of ensuring the security of its members, NATO made a fairly significant contribution to maintaining a state that was not very bellicose and, at the same time, contributed to winning a competition that neither the ideology, nor the institutions, and ultimately, nor the economy of the opposing camp were able to sustain. In the same vein, we can say that there was also a cultural conflict and clash of civilizations, determined by the differences in the way essential rules were respected at both domestic and international levels.

I. The appearance of the North Atlantic Alliance against the backdrop of the need for cooperation

The North Atlantic Alliance emerged in the context of evolving complex and varied threats that jeopardized the security of its member states, marking a crucial point in the dynamics of international relations. In an era characterized by escalating post-war tensions and intensified geopolitical rivalries, the alliance became a pillar of stability and security in Europe and North America. NATO's foundation is firmly anchored in the principle of ensuring collective security, which emphasizes solidarity and cooperation among its members. In institutional terms, NATO can be conceptualized as an interconnected system, designed to respond cohesively and efficiently to external threats. A crucial element of NATO's evolution has been the strengthening of the military capabilities of its member states, in a concerted effort to address complex and diverse threats. This consolidation has been achieved through investments in military infrastructure, equipment modernization, and the promotion of interoperability among the armed forces of member states.

In addition to the military dimension, cooperation in the field of information and joint strategic planning has been promoted, thereby facilitating the exchange of expertise and coordination of actions among its members. This expanded collaboration has increased the efficiency and effectiveness of the alliance in the face of security challenges. An important aspect of NATO's evolution is its adaptability to changes in the geopolitical environment and the emergence of new threats, such as terrorism and cyber threats. The alliance has revised its strategies and priorities to address these evolving challenges, maintaining its relevance and effectiveness in the fight for security.

1.1 Anarchy-catalyst for the formation of the Alliance

In a state of anarchy, actors in the international system must rely on their own capabilities and structures, and the way this is achieved is through self-help (Waltz Kenneth, Theory of International Politics, Polirom, Iasi, 2006, p. 151). In a state of anarchy, even though it entails a major risk of failure, organizational costs are relatively low. In contrast, in a hierarchical order, risks are reduced or ideally avoided altogether. At the same time, the costs of maintaining such an order are much higher, and the means of control become objects of contention. On the other hand, in a hierarchical order, freedom is limited, which means that if a greater degree of freedom is desired, insecurity must be accepted along with it (Waltz, Kenneth. Theory of International Politics. Polirom Iasi, 2006, p. 153).

The question that arises is why does the state of anarchy not lead to a system dominated by complete chaos?

1.2 Self-help- a key principle of state survival

We can say that the state of anarchy is not equivalent to chaos, but arises from the fact that there is no superior authority to the state anywhere. This "disorder" is neutralized by each state's desire to exist, a concept that Kenneth Waltz defines in his work "Theory of International Politics" as self-help. Specifically, he argues that: "The international system is based on 'self-help',"(Waltz K. Theory of International Politics p.153) this means that states, as actors in the international system, have self-help as their only means of ensuring security, each making efforts not for the pursuit of their own good, but rather with the aim of protecting themselves from others. (Waltz K. Theory of International Politics p.151). The principle guiding action is self-help, but when faced with the possibility of cooperating for mutual gain, states feeling insecure question not whether both will "win," but rather who will win more, raising the issue of ensuring their own security.

Kenneth Waltz's theory of the international anarchic system provides a useful perspective for understanding how states act to ensure their security in an environment characterized by the absence of a central authority and a clear hierarchy. According to Waltz, in such a system, states are driven by their desire to protect their survival and national interests, primarily seeking to maximize their own security through their capacity for self-help. In this context, NATO represents an expression of the concept of self-help, being founded on the principles of solidarity and collaboration among member states to ensure collective security.

1.3 The strengthening of military capabilities – an attribute of self-help

An essential aspect of the concept of *self-help* within NATO is *the strengthening of the military capabilities* of member states. This involves investments in military infrastructure, equipment modernization, and the development of operational capacities to address a wide range of security threats, from conventional military aggression to asymmetric threats such as terrorism and cyber warfare.

Moreover, within NATO, self-help is manifested through *collaboration* and *operational coordination* among member states in *joint military actions* and training exercises. Collaboration allows member states to maximize their efficiency and effectiveness against common threats and to enhance their capacity for rapid response in crisis situations. As a relevant example of the concept of self-help, NATO conducts military operations in areas such as Afghanistan and the Western Balkans. In these missions, member states have collaborated to stabilize and rebuild these regions, combating security threats and promoting democratic values and the rule of law.

Another important aspect of self-help within NATO is the *exchange of information* and *operational coordination* to counter terrorist and hybrid threats. Member states share expertise and security resources to detect and prevent terrorist attacks and to counter the subversive and disinformation actions of adversaries.

In conclusion, the concept of self-help in *Kenneth Waltz's* theory, applied within NATO, constitutes a central element in understanding how state security is ensured in an anarchic international environment. Through the strengthening of military capabilities, operational collaboration, and exchange of information, NATO member states maximize their efficiency and effectiveness against external threats, thus demonstrating the importance of solidarity and cooperation in promoting collective security and international peace.

John Mearsheimer argues that states *can ensure their security by increasing their power*; specifically, he asserts that: "States seek to maintain their territorial integrity and the autonomy of their domestic political order. Survival trumps the other motives because once a state is conquered, it is impossible for it to pursue any other goals. States can pursue other goals, to be sure, *but security is their most important objective*." (Mearsheimer John, The Tragedy of Great Power Politics, Antet Publishing House, Bucharest, 2003, p.27)

1.4 Balance of power – a contributing factor to the founding of NATO

The *balance of power* is originally an anti-hegemonic project that has been operating since the beginning of the formation of the system of sovereign states as a form of institutionalized management of international security. The fundamental logic it operates on is that of a relative equilibrium between at least two opposing camps, acting based on the politics of power redistribution within the system, relying on reciprocal deterrents primarily of a military nature. (Mearsheimer John, The Tragedy of Great Power Politics, pp.103-104) The balance of power is a distinct political theory in international politics, yet there is still no generally accepted definition. (Waltz K. Theory of International Politics p.166) The purpose of this theory is to explain the outcomes of states' actions, rather than their immediate actions themselves. (Waltz K. Theory of International Politics p.174)

The balance of power is formed recurrently, with states tending to mimic the successful policies of other states. The failure of certain states to conform to the successful practices of others is explained by the effects of forces outside the scope of interest of the theory. (Waltz K. Theory of International Politics pp.174-175)

Kenneth Waltz argues that the international system is "systemically dominated," with states' behavior dictated by structure. The structure does not change when new states enter the system, nor when the system has a homogeneous structure (considering the case where all members are democracies), because the interactions between states say nothing about the structure of the system. (Buzan Barry and Little Richard, International Systems and World History, Polirom Iasi, 2003, pp.56-57). The international framework is anarchic in nature and dominated by a struggle for survival, leading us to a security dilemma that will find expression in an overall system where each helps themselves. (Guzzini Stefano. Realism and International Relations. European Institute, Iasi, 2000, p.242.) *Waltz's balance of power theory is based on the idea that on the international stage, states pursue the same goal, which is ensuring survival*, but the existence of balance also aims at *preserving the system by balancing it*. It can also be seen as evidence of interaction between major powers and their ability to adapt to the variable distribution of power, while also showing the ease with which they change partners.

By balance of power, stability within a system composed of several autonomous forces is designated; whenever the equilibrium within the system is disturbed by an external force, there is a tendency to restore order within the system. The balanced distribution of power in the system is usually made either by a great power or by a group of great powers, but the desire for power of the states makes the balance of power no longer strictly used for defensive purposes, so the balance exists for the purpose of power maximization and along with this, policy alliances are formed in response to threats. (Walt Stephen. The Origins of Alliances. European Institute Iasi, p. 56.)

Faced with an external threat, states are compelled to react; they either balance or align. Thus, two hypotheses emerge regarding how states select their alliance partners, either in favor of the threat or against it. This results in two worlds: a world of balancing and a world of alignment. In cases where balancing is more common than alignment, states are more secure, as their aggressors will be met with combined opposition. However, if alignment is the dominant tendency, security is reduced, as successful aggressors will attract allies, bolstering their power and diminishing that of their opponents (Walt Stephen. The Origins of Alliances. p. 57)

Hans Morgenthau, one of the most renowned theorists of international relations, believes that the best way to ensure security is through the *balance of power*, seen as *a defining instrument for nations whose independence and existence are threatened by the disproportionate rise of other nations*. (Morgenthau Hans J. Politics Among Nations. Polirom Iasi, p. 241.) This problem arises possibly because the natural state of states is a state of war. However, this does not mean that war constantly occurs, but rather that each state decides for itself whether to use force, indicating that war can break out at any moment. (Waltz, Kenneth, p. 147).

More specifically, realists in conditions of anarchy do not ask themselves "if the next war will occur," but rather "when." (Ungureanu Radu Sebastian, International Relations Book, Polirom Publishing House, Iasi, p.103) According to Hans Morgenthau's theory, *the balance of power represents a central concept in the study of international relations and in the management of national security*. Morgenthau believed that power is a fundamental component of international politics and that states pursue their national interests through the use and maintenance of power equilibrium in the international system. In Morgenthau's view, the balance of power aims to prevent any single power from dominating the international system and, implicitly, threatening the survival of other states. This equilibrium is considered essential for maintaining stability and security within the international community. Therefore, states are motivated to strengthen their military capabilities and form alliances to maintain this balance and protect their own interests.

A concrete example of the application of the *balance of power* concept is represented by the *evolution of NATO* in the post-Cold War period. Following the collapse of the Soviet Union and the dissolution of the communist bloc, security in Europe faced new challenges and threats. NATO's expansion eastward, towards former Warsaw Pact member states, was perceived as a strategic move to maintain a balance of power in the region and to strengthen collective security. By including these states within the alliance, NATO contributed to deterring aggression from other state or non-state actors and to consolidating its position within the international system. Thus, NATO member states acted in accordance with the theoretical principles of the balance of power, seeking to maintain a power equilibrium in the region and prevent any hegemonic tendencies. Moreover, the consolidation of military capabilities and mutual support among NATO member states constituted a crucial aspect of applying the balance of power concept. Through these measures, the alliance managed to enhance its deterrence and response capabilities against potential threats, contributing to increased stability and security in the region.

However, it is important to acknowledge that the application of the *balance of power* concept is not without *challenges* and *controversies.* Some critics argue that emphasizing power equilibrium can lead to the escalation of conflicts and hegemonic competitions between states, generating instability and insecurity within the international system. However, through this concept, states are motivated to maintain their power balance in the international system, thereby contributing to increased stability and security within the international community. The implementation of the balance of power concept within NATO and other international organizations is crucial for promoting global peace and security.

1.5 Balancing as protection against threat

According to *balancing* behavior, states form alliances to protect themselves against other states or coalitions whose superior resources pose a threat, and they choose to balance for two reasons. The first would be risking their survival if they fail to confront a potential hegemon before it becomes too powerful. The second would be that collaboration with the weaker party increases the influence of the new member within the alliance, as the weaker party needs greater assistance. (Ungureanu Radu Sebastian, International Realations Book, p.58) In a balancing world, states that pose a threat will provoke other states to ally against them, while those seeking to dominate other states will attract significant opposition.

In this balancing world, credibility is not very important because the allies of a state will resist threats, pursuing their own interests as they expect others to adopt the same behavior, reducing the fear of defecting. Once balancing predominates and aggressive behavior has been discouraged, strong resistance and political communication based on goodwill and moderation can be anticipated, considered most effective in a balancing world. (Walt Stephen. The Origins of Alliances. European Institute Publishing, Iasi, p. 68). This even though state decision-makers fear that potential allies may defect to the side of the stronger.

Balancing takes two specific types of action: the *first* is when, in the case of a conflict with a balance tilted in favor of a revisionist state or group of states, *an actor may choose to ally with a weaker state to balance the revisionist state*, within the alliance, however, also considering the cost-benefit ratio and the capabilities of the ally. (Miroiu Andrei and Ungureanu S., International Relations Book, p. 204) *The second* situation is that of balancing with the aim of fulfilling the *role of a balancing factor*; it usually occurs before the outbreak of a conflict with the goal of maintaining the balance of power. Here, the perception of a state is very important, specifically its ability to maintain equilibrium. At the same time, it largely determines the structural order of the system after the conflict is resolved. (Miroiu Andrei and Ungureanu S., International Relations Book, p. 204)

1.6 Alignment as a mode of survival

Alignment behavior can be seen as the easiest way to emerge as a winner from a conflict and at the same time to share the "gains" (economic, territorial, etc.) with other allies/winners. (Thomson Scott W. in The Origins of Alliances. European Institute Publishing, Iasi, p.59) More specifically, *alignment refers to the action of attaching a state to the stronger side* or perceived stronger side in a given conflict, based on two assumptions. The first assumption is that states aim for survival, and in this case, a state allies itself with another, usually a revisionist one. The second assumption involves gaining benefits from the conflict, with states aligning themselves with a power in the international system that they see as a potential victor. Alignment policy is not only an option for minor powers but also for major powers.

Alliances are a necessary function of the balance of power and operate within a multilateral system, with essential goals of adding to the power of another nation or preventing the adversary from doing the same.

Starting from Walt's question: “Do states seek allies to balance against a threat or align themselves with the most threatening state’?” (Walt Stephen. The Origins of Alliances, p.41) we can reflect on whether NATO is an alliance in response to a threat. We can say yes, based on the founding treaty of the alliance, which tells us that: 'The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security. (http://www.nato.int/cps/fr/natolive/official_texts_17120.htm)

Conclusions

In light of the evolution of international threats, NATO remains a central element in the architecture of global security, playing a crucial role in maintaining stability and security in Europe and North America. Within the balance of power, the Alliance plays a fundamental role in a rapidly changing security environment. An important aspect of NATO's evolution is its geographical and operational expansion. By adding new member states from Central and Eastern Europe, the alliance has strengthened its presence and influence in regions that were previously vulnerable to external threats. This expansion process has consolidated security and stability in Europe and promoted integration and cooperation between former communist states and Western European countries. At the same time, adapting to contemporary threats is a crucial aspect of NATO's evolution. In the current context of hybrid and cyber threats, the alliance must strengthen its capabilities for detecting, preventing, and countering these types of threats. Thus, NATO needs to invest in advanced cybersecurity technologies, develop integrated strategies to combat disinformation, and consolidate cooperation with other international organizations and relevant actors in the field of cybersecurity. Additionally, strengthening partnerships with other international and regional organizations is essential for addressing transnational challenges effectively and promoting sustainable global security. Through collaboration and coordination with organizations such as the United Nations, the European Union, and the Organization of the South Atlantic Treaty, NATO can amplify the impact of its actions and promote lasting solutions to conflicts and threats to global security.

Despite current challenges and threats, NATO remains a central actor in efforts to maintain international stability and security. By continuously adapting to the new dynamics of global security and strengthening partnerships and collaboration between member states and other relevant organizations, the alliance can play a significant role in promoting peace and security in the 21st century. It is essential for member states to intensify their efforts to enhance the alliance's capabilities and to promote democratic values and the rule of law worldwide, thereby contributing to the achievement of NATO's objectives and principles.

BIBLIOGRAPHY:

1. Buzan Barry and Little, Richard. International Systems and World History. Polirom Publishing House, Iasi, 2003
2. Constantinescu Mihnea. In Eugen Preda's "NATO-A Brief History." Published by Cultural Foundation Magazine Historia, Bucharest, 1999
3. Fidler Jiri and Mares Petr. History of NATO. Published by European Institute, Iaşi, 2005
4. Guzzini Stefano. Realism and International Relations. European Institute Publishing House, Iasi, 2000
5. Mearsheimer,John. The Tragedy of Great Power Politics. Antet Publishing House, Bucharest, 2003
6. Miroiu Andrei and Ungureanu, Radu Sebastian. International Relations Book. Polirom Publishing House, Iasi
7. Morgenthau Hans J. Politics Among Nations. Polirom Publishing House, Iasi
8. Thomson Scott W. Cited in Walt Stephen. The Origins of Alliances. European Institute Publishing, Iasi
9. Walt Kenneth N. Theory of International Politics. Polirom Publishing House, Iasi
10. Walt Stephen. The Origins of Alliances. European Institute Publishing, Iasi
11. Waltz Kenneth N. Theory of International Politics. Polirom Publishing House, Iasi, 2006
12. http://www.nato.int/cps/fr/natolive/official_texts_17120.htm

1053477-3045-1396-24-08

INVOLVEMENT OF YOUTH IN POLITICAL LIFE – A VECTOR OF DEMOCRATIC RESILIENCE

Veronica DUMITRAȘCU, PhD.
Researcher, Euro-Atlantic Resilience Center, Bucharest, Romania
E-mail: veronica.dumitrascu@e-arc.ro

Abstract: *In the context of the electoral year, an analysis of the political participation of young people is necessary because it may lead to observations that could contribute to the democratic process of voting. The participation of young voters is indicative of their engagement in promoting democratic values. The importance of the topic is relevant in the context of the 2024 elections, especially because it highlights a current and ever-present issue at the societal level, with implications at the national, regional, and/or international levels. What implications could youth political participation have for a healthy democracy? What indicators could explain youth voter absenteeism and/or their declining turnout? Why are they no longer involved in "citizen affairs"? The subject underscores the importance of the political participation of young people as an indicator of an inclusive and resilient society.*

Keywords: *democratic resilience, political participation, youth participation, civic engagement, vote turnout, youth policies*

Introduction

The concept of democratic resilience serves as a benchmark for conducting electoral analyses reflecting the behavior and perceptions of the population. Burnell and Calvert describe democratic resilience as "a commitment to democratic ideals, despite hostility towards prescribed values and norms and indifference towards many elements of society." Analyzing the concept from a broader perspective, Merkel and Luhrmann (2021, 872) define democratic resilience as "the ability of a political regime to prevent or react to threats without losing its democratic character".

Voter turnout is one of the key indicators of democratic resilience. Voter turnout stands as one of the most important factors regarding the "democratic health" of a state. One of the most important indicators for an inclusive democracy is voter turnout or the percentage of eligible voters who cast their ballot in a given election (Hubdialer, n.d).

High voter turnout shows that citizens are actively engaged in democratic processes and the political life of society. Low voter turnout indicates a lack of interest in politics and may be a sign of distrust in political authorities and democratic processes. Low support of the population may be a sign for officials to implement some changes at the political and governmental levels.

As some analyses (Hubdialer, n.d) show, „older, more educated and higher-income-earning people are more likely to vote than younger, less educated people and people with lower incomes”.

The paper tries to emphasize the engagement's importance of the young people in electoral processes and their implication in political life as a positive sign of democracy.

European democracies have witnessed a decline in voter turnout since the mid-1980s and post-communist countries have experienced a massive drop in voter turnout after transitioning to democracy (Deželan 2023). A 2020 survey recorded one of the lowest voter turnouts since 1990, below 32% (Burciu 2024).

1. The decline in vote turnout of the young people

The engagement of young voters in electoral processes assures an equilibrium in society according to democratic norms and values and may promote intergenerational stability. As future leaders who may be involved in political decisions, younger voters' voices could count as promoters of democracy.

Studies (Deželan 2015 cited in Galstyan, 2019) show a decline in voter turnout, political affiliation, and trust in political institutions among young people. "Today's youth are less involved in institutional politics than other age groups and also less than cohorts of young people from decades ago" (Deželan 2023).

Some analyses indicate that the absence or decrease in youth participation in political life signifies their low expectations from the government, considering the relatively few initiatives focusing on projects targeting young people.

Why do we focus on the young segment of the population in our study? Because "age is a strong predictor for a wide range of beliefs, knowledge, and behaviors, and because adolescents and young adults tend to change their behavior more rapidly when external conditions change" (Bădescu, G. et al 2019). Furthermore, the behavior of young people can influence a series of other decisions and actions regarding the political life of society. Zukin et al. (2007) indicate that age, along with income and education, is one of the significant predictors of voter turnout, pointing to "an alarmingly low voter turnout among young people at various levels and in different regions and countries"(Bădescu, G. et al 2019).

It is important to track what other predictors could explain the decrease in youth voter turnout, especially in recent years. Additionally, it would be interesting to analyze the long-term consequences of this phenomenon and what they imply for the stability of democracy.

There are some factors that may explain the decrease in young vote turnout, such as socio-economic background, educational factors, accessibility to voting centers, access to information, etc.

An article from the New York Times (Symonds 2020) shows that there are some themes in political science that "may explain the gap for young voters":

1. „Voting is a habit formed over time and, with time, people turn from „habitual nonvoters" to „habitual voters";
2. Opportunity cost. Young adults may have less flexible employment schedules or less financial cushion to take time off to vote;
3. A lower participation in the electoral process may be followed by intense active participation in other forms of activism, such as signing petitions, protests, boycotts, or increased activity of social media as a platform for political engagement, according to research conducted by the Stockholm-based International Institute for Democracy and Electoral Assistance" (Symonds 2020).

The same research from the International Institute for Democracy and Electoral Assistance shows that „young people may be motivated not to vote because their demands are not being addressed by the political parties or leaders competing in elections" (Solijonov 2006, 40). In other words, political officials may not properly communicate with young people in their terms and the proper political messages may not arrive to them.

On the other hand, the decrease in young people's vote may be explained through vote apathy. Many young people may not be interested in politics because they tend to think that their voice is not heard and respected by the decision-makers, so they begin to lose trust in traditional institutions of governance.

A way to increase youth involvement in democratic processes is to encourage their participation in civic and political life. In future studies, comparative analysis could help us to see regional disparities related to youth political engagement, in order to outline measures that could reduce these differences. For example, a study conducted in a Nordic country where democracy is at its highest levels (e.g., Norway with a democratic index score of 9.81(The Economist Intelligence Unit, 2024) and a score of 10 regarding political participation and political culture (The Economist Intelligence Unit, 2024), compared to Romania which, according to the same report, has a democratic index score of 6.45, a political participation score of 5.56, and a political culture score of 3.75, or Bulgaria with a democratic index score of 6.41, a political participation score of 5.56, and a political culture score of 4.38 (The Economist Intelligence Unit, 2024) compared to a country with a low democratic index (see above example).

2. Civic and political engagement of the young people

Besides analyzing predictors, it is interesting to track the civic engagement of young people. Civic engagement refers to all forms of actions, from associations, volunteering, protests, voting, etc. Civic engagement means "to promote the quality of life in communities through political and non-political processes" (Ehrlich, 2000). It "covers everything from voting to contributing to acts of charity, to participating in political rallies and marches" (Berger cited in Erkman; Amna, 2012). One objective of the study would also consider the commitment/involvement of young people in political life through signing petitions, volunteering for various organizations and political parties, participating in protests and boycotts, etc. A study from 2019 (Burciu 2024) shows that 62.3% of young people aged 18 to 29 were not interested in politics at all, and 80% of the same age group did not participate in any political activity (e.g., signing petitions, participating in protests, volunteering, etc.). The same study underlined the fact that „Romania has one of the lowest rates of positive opinions about democracy in the EU, with approximately 20% believing that "democracy is not a good form of government" and over 23% agreeing that "in some circumstances, dictatorship is better than democracy" (Burciu 2024).

It's interesting to analyze the link between online and offline participation of young people in political life.

There were different studies (Della Porta, Mosca, 2005; Burean and Bădescu, 2014, 7) that showed a link between internet activism and offline participation.

The Internet is „a catalyst for protesting" and a medium where people interact and share their ideas, increasing the potential for engagement in protests" (Dumitrașcu 2020).

Some studies showed that people engaged in online networks were also involved in offline protest actions, as Mercea (2012) claimed, the online activities coincide with offline activities, as Hirzalla and van Zoonen (2009) showed, or that "online activism is a precursor of offline activism", as Harlow Summer and Dustin Harp (2011) concluded.

The Cultural Consumption Barometer from 2022 (Croitoru et al. 2022) showed that „young people, especially those who spend a lot of time on the internet and social media, have a lower level of social trust (even in the people in their neighborhood or community where they live), exhibit lower levels of tolerance, and are almost disinterested in social or civic participation". The Barometer claimed that „the impact of the cultural consumption on democracy occurs through much more complex mechanisms that involve personal and social characteristics or differentiated consumption patterns" (Croitoru et al. 2022).

The absence of youth participation in political life also affects the process of representing young people in basic institutions. As a study suggests, "the simple fact that 'if you vote, you don't matter' (Martin 2012, 107) indicates that low youth participation in political life means they have low expectations from the government" (Deželan 2023), they no longer trust basic institutions (Government and Parliament). According to the World Values Survey, between 2017-2022, in Romania, the trust of young people up to 29 years old in the Government was 14%, six percentage points lower than in 2005-2009, when it was 21%. Those in the 30-49 age group had a 15% trust in the Government in the same years (2017-2022), and those in the over 50 age group had a 20% trust, six percentage points higher than the young.

As Deželan (2023) shows, young people are underrepresented in democratic processes. Factors leading to low participation may include "the changing relationship between young people and the political sphere, political socialization, and key events during socialization, as well as changing civic norms among young people, which are also related to how we define political participation."

As some studies (Burciu 2024) point out, the current legislation in Romania "does not provide for mechanisms dedicated to involving young people in decision-making processes, not even an advisory role on issues that would directly influence them, with many of their requests rarely included on the executive agenda."

The electoral commitment of young people is also linked to the methods and access to information (online, from the press, radio, and TV). The information media of young people also depends on the environment of origin, as well as the circle of friends. Young people tend to spend a significant amount of time online, being much more willing to get their information from the internet. This leads to their vulnerability to misinformation from the online environment, propaganda, and fake news circulating on social networks. As Burciu (2024) enhanced, social media platforms are a proper medium for malicious narratives. „Young people, who represent the largest audiences on some of the platforms (..) are disproportionately exposed and particularly vulnerable to radicalization" (Burciu 2024, 21).

Identifying the mechanisms and processes of misinformation that influence young people, as well as correlating them with political participation and the voting intentions of young people are important issues that should be analyzed in future studies.

Social media platforms continue to provide an effective medium for malicious ideas to be disseminated and amplified and for their exponents to be popularized, via online echo chambers, algorithms prioritizing user engagement, as well as the anonymity emboldening individuals to express themselves without the fear of rejection and consequences of non-digital spaces

3. Youth policies for encouraging young people to vote in Romania

More measures, legislation proposals, and programs for encouraging young people to vote should be implemented on a larger scale.

As the „Youth Policies in Romania" report from 2019 mentioned, „there is no information on existing legal frameworks and key policy programs, projects or initiatives enabling or encouraging young people to participate in political processes electronically" (The Youth Wiki is Europe's online encyclopedia 2019).

The ability to engage young people in political activities should be developed from primary school.

The children should be informed by school and by their educators about their democratic rights and their democratic values.

There should be curricula and courses available in primary school to enhance pupils' skills to participate in political debates and political decisions. Nowadays there are no guidelines, handbooks, or didactic materials to support educators in teaching children about their democratic rights and how to engage in political activities.

More than that, „no information is available on top-level policy on partnerships between formal education providers, youth organizations and youth work providers".

Another important point in stimulating young people to vote is to encourage debates and reforms in the field of youth participation. The development of programs and projects for young people to arouse their implication in political debates is the great importance for democratic resilience.

As the report from 2019 underlined, even if some projects promote and contribute to the development of civic and social competencies, the data are not monitored and their outcomes and results aren't published.

It's important „to encourage youth involvement in decision-making processes to facilitate their understanding of democratic mechanisms" (The Youth Wiki is Europe's online encyclopedia 2019) and to develop special policies regarding transparent public communication between young people and political decision-makers. The increase of youth motivation to participate in community life through initiatives and debates and to promote interest in volunteering opportunities are important for the development of democratic resilience.

The National Youth Strategy has five main pillars/key areas of intervention: „1) culture and non-formal education; 2) health, sports, and leisure; 3) participation and volunteering; 4) employment and entrepreneurship; 5) the social inclusion of young people" (The Youth Wiki is Europe's online encyclopedia 2019).

According to EU Youth Policy Cooperation, it is important to attract young people to different cultural and educational programs: for example, to establish the link between EU Youth policies and EU programs (such as Erasmus + and European Solidarity Corps). EU Youth Strategy focuses on three attributes: engage, connect, and power. It promotes equal access to opportunities and information.

On the EU Youth Policy agenda there are also other considerations:

- "To Improve cross-sector cooperation across policy areas, including through an EU Youth Coordinator, to give youth a voice in shaping EU policies
- Track EU spending on youth;
- Launch a new and more inclusive EU Youth Dialogue, with a focus on youth with fewer opportunities;
- Remove obstacles to and facilitate volunteering and solidarity mobility;
- Implement a youth work agenda to increase recognition of non-formal learning" (European Commission 2018).

At the national level, cooperation between policy-making and research institutions, funding youth policy, organizing activities, programs, and curricula to stimulate the participation of young people in political and civic activities, offering information services for young people in terms of voting, „ensuring the representation of Romania to the national and international events in the field of youth" (The Youth Wiki is Europe's online encyclopedia 2019), are important measures to encourage political engagement of young people.

Conclusions

The political participation of young people in democratic processes is essential for building an inclusive and resilient society. The article shows the importance of vote turnout as the key indicator of democratic resilience, the factors that determine the decline in vote turnout of young people, and the implications of their engagement in civic and political life.

The decrease in vote turnout of young people has multiple consequences concerning the political life of societies. Building inclusive and sustainable civil society through political engagement of young people took to a resilient society.

Engaging young people in the electoral process promotes stability in society and an inclusive democracy.

The absence of youth participation in political life also affects the process of representing young people in basic institutions. So, a focal point of every country's strategy is to encourage youth involvement in decision-making processes, to take into consideration the youth „voices” and to stimulate young people to vote.

BIBLIOGRAPHY:

1. Bădescu, G. et al. 2019. Studiul despre tinerii din România. Friederich Ebert Stiftung. https://library.fes.de/pdf-files/bueros/bukarest/15294.pdf
2. Burciu, D. 2024. Youth radicalizationin Romania. How Far- right actosr target Romanian Youth ahead of the 2024 election. Global Focus Center. https://www.global-focus.eu/wp-content/uploads/2024/02/Youth-Radicalisation-in-Romania.pdf
3. Burean, T. and Bădescu. G. (2014). Voices of discontent: Student protest participation in Romania. Communist and Post-Communist Studies 47 (3-4): 385- 397.
4. Calvert and Burnell. 1999. The Resilience of Democracy. London, Frank Cass.
5. Croitoru et al. 2022. Cultural Consumption Barometer 2022. Cultural participation and democratic perspectives, https://www.culturadata.ro/barometrul-de-consum-cultural-2022-participare-culturala-si-perspective-democratice/
6. Della Porta, D. and Mosca L. (2005). Global-net for Global Movements? A Network of Networks for a Movement of Movements. Journal of Public Policy 25 (I): 165– 190.
7. Deželan, T. 2023. Young people'sparticipation in European democratic processes. How to improve and facilitate youth involvement. Policy Department for Citizens’ Rights and Constitutional Affairs.
8. Dumitrașcu V. 2020. Online and offline activism. Literature review. Revista Universitară de Sociologie. Year XVI, no. 2/2020
9. European Parliament, Study. Young people's participation in European democratic processes. Policy Department for Citizens’ Rights and Constitutional Affairs. Martie 2023.
10. European Comission. Engaging, Connecting and Empowering young people: a new EU Youth Strategy, Brussels, 22.5.2018.
11. Hirzalla, F. and van Zoonen L. V (2009). Beyond the online/ offline divide: How Youth’s online and offline civic activities converge. Social Science Computer Review 29 (4): 481-498.
12. Hubdialer. What is voter turnout and why does it matter for democracies? https://www.hubdialer.com/glossary/what-is-voter-turnout/
13. Martin, A.J. 2012. Resilience and learning. In N.M. Seel (Ed.). Encyclopedia of the Sciences of Learning. New York: Springer.
14. Merkel, W., Luhrmann. 2021. Resilience of Democracies: Responses to Illiberal and Authoritarian Challenges, CEU Democracy Institute, https://democracyinstitute.ceu.edu/articles/wolfgang-merkel-and-anna-luhrmann-resilience-democracies
15. Solijonov, A., Voter Turnout Trends around the World, International Institute for Democracy and Electoral Assistance, 2006.
16. Symonds, A. 2020. Why Don’t Young People Vote, and What Can Be Done About It?, https://www.nytimes.com/2020/10/08/upshot/youth-voting-2020-election.html
17. Summer, H., Harp, D. 2012. Collective action on the web. A cross- cultural study of social networking sites and online and offline activism in the United States and Latin America. Information, Communication and Society 15 (2): 196-216
18. The Economist Intelligence Unit. 2024. Democracy Index 2023. Age of Conflict.
19. The Youth Wiki is Europe's online encyclopaedia in the area of national youth policies. Youth policies in Romania, 2019. https://national-policies.eacea.ec.europa.eu/sites/default/files/2021-06/Romania_2019.pdf
20. World Values Survey. Online Data Analysis. https://www.worldvaluessurvey.org/WVSOnline.jsp

21. Zukin et al. 2007. A New Engagement? Political Participation, Civic Life, and the Changing American Citizen. Perspectives on Politics, Vol. 5, No. 2 (Jun., 2007), pp. 379-380

1053477-3045-1396-24-09

WEATHERING THE DISINFORMATION STORM IN 2024'S ELECTORAL CONTEXT

Daniela MUNTEANU, PhD. candidate
Euro-Atlantic Resilience Centre, Ministry of Foreign Affairs,
PhD candidate, National University of Political Studies and Public Administration, Bucharest, Romania
daniela.munteanu85@gmail.com

Abstract: *The present study explores the effectiveness of the current framework set in place at Euro-Atlantic level to ensure societal resilience to disinformation. We delve into whether or not European societies are equipped to manage information manipulation and its effect on democracies in the context of the 2024 elections. Through a comprehensive analysis, the article examines the policies and strategies deployed to combat disinformation throughout the past decade, evaluates their effectiveness, and assesses their impact on public trust and electoral integrity. From a methodological standpoint, the paper identifies trends in disinformation tactics and their evolution, connecting the dots between disinformation and its effects on democratic resilience in a longitudinal approach. It discusses the collaborative efforts between governments, tech companies, and civil society in safeguarding democratic values against the backdrop of increasing digital manipulation. The article continues by offering insights into the most notable measures aimed at bolstering resilience to disinformation for safeguarding democratic institutions and societal cohesion. The concluding analysis delves into hurdles that need to be overcome when it comes to implementing the frameworks that have been put forth by the EU, the organisation that has championed resilience building in many aspects – societal and democratic at the forefront – throughout the past years.*

***Keywords**: disinformation, democratic resilience, societal resilience, electoral processes;*

Introduction

2024 is the year with the largest number of elections in history: it will test the democratic prowess of over 40 billion people in more than 70 countries. We are traversing, therefore, a pivotal moment in the global political landscape, marked by a series of critical elections across diverse geopolitical contexts. These electoral processes not only reflect the internal dynamics and challenges of individual countries but also have significant implications for international relations, global governance, and the promotion of democratic values.

Eagerly and consistently pursued in many corners of the world, democracy has come to be readily equated with free elections. In the current digital age, is it still possible to interlink the two, ignoring the nuances of how the information space contributes to swaying hearts and minds? An in-depth analysis of the information space during the past decade shows that viral information circulating on social media influenced whether most of us cast the ballot or not, voted right, centre or right (Colomina, Margalef, and Youngs 2021). Democracy, as a form of government in which power is vested in the people and exercised by them directly or through freely elected representatives is heavily reliant on the same hearts and minds that autocratic regimes are trying to win over for their own geopolitical gains.

The concept of ”democracy” – originating from the Greek words "dēmos" (people) and "kratos" (power, rule), meaning "rule by the people" (Dahl, Shapiro, and Froomkin 2024) – is characterized by principles of political equality, where each adult citizen has a say in the decisions that affect their lives, typically through voting in elections. Moreover, it is also characterized by features such as freedom of assembly, association, speech, religion, personal property rights, citizenship, consent of the governed, voting rights, protection from unwarranted governmental deprivation of life and liberty, and minority rights (Christiano and Bajaj 2022). Ironically, it is at the very roots of democracy that malign illiberal actors attack. They manipulate public discourse and general opinion in a relentless attempt to determine citizens to use their freedom of speech and assembly, minority rights and religion as weapons against their own safety, health, liberties and, at times – as seen during the pandemic –, even lives. Disinformation – under its many facets – is an extremely effective tool to employ: inexpensive (from a cost-benefits perspective), liable to operate at the legal threshold, easily deniable when it comes to primary sources of narratives and spreaders.

What are, therefore, the lessons that we can learn from looking at how disinformation evolved in the digital era and how can we limit its nefarious impact? Is there a set of tools that have proven to work effectively in managing disinformation and its consequences? Are the regulatory measures and frameworks in place sufficient to help us fare through the biggest election year in history?

We attempt to offer some food for thought and possible solutions by employing a research methodology in which we analyse official and strategic documents, academic literature and existing studies on democratic and societal resilience in order to map out the conceptual contours of what we broadly comprise under the umbrella-term of ”disinformation”. We employ a qualitative analysis of the policies and strategies devised by relevant actors, such as the EU and NATO, in order to handle the negative impact of the phenomenon on Euro-Atlantic societies and bolster societal resilience to disinformation. We assess the feasibility of the measures undertaken by international organisations and we conclude by highlighting challenges which remain to be overcome in a resilience-building approach to the threats posed by disinformation to our democratic societies.

I. Navigating Disinformation in Democratic Societies – an attempt to tame the concept

In the era of digital communication, the proliferation of disinformation and various forms of information manipulation pose significant challenges to the integrity of public discourse, democratic institutions, and national security. This section provides a comprehensive framework for understanding disinformation, drawing on definitions from key international bodies such as the European Union (EU), the North Atlantic Treaty Organization (NATO), and scholarly research. It also explores related concepts including misinformation, malinformation, information operations, and foreign information manipulation and interference, highlighting the nuances and implications of each category.

I.1 Disinformation: Definitions and Perspectives

NATO views disinformation as the deliberate creation and dissemination of false or manipulated information with the intent to deceive or mislead. The word “disinformation” is commonly used as an umbrella term to represent a wide range of tactics, techniques and procedures, which are described by NATO as “hostile information activities.” These activities seek to deepen divisions within and between NATO member countries and ultimately weaken the Alliance (NATO 2023a).

The EU defines disinformation as ”verifiably false or misleading information that is created, presented, and disseminated for economic gain or to intentionally deceive the public, and which may cause public harm” (European Commission 2018, 1). This definition emphasizes the deliberate nature of disinformation and its potential to inflict harm on society. Nevertheless, there are several dimensions to what we broadly deem to place under the concept of ”disinformation”, and the 2020 European Action Plan brings about the needed nuance in an official document: ”*misinformation* is false or misleading content shared without harmful intent, though the effects can still be harmful, e.g. when people share false information with friends and family in good faith; *information influence operations* refer to coordinated efforts by either domestic or foreign actors to influence a target audience using a range of deceptive means, including suppressing independent information sources in combination with disinformation; *foreign interference in the information space*, often carried out as part of a broader hybrid operation, can be understood as coercive and deceptive efforts to disrupt the free formation and expression of individuals' political will by a foreign state actor or its agents" (European Commission 2020, 18).

The definitions provided by the European Union are rooted in academic research, making use of seminal work, such as that of Wardle and Derakhstan, who have also established *malinformation* as a side of disinformation. In their work *Information disorder: Toward an interdisciplinary framework for research and policy making*, the two authors define malinformation as the use of factual information in a way that is intended to cause harm to an individual, social group, organization, or country (Wardle and Derakhshan 2017, 20). Unlike misinformation and disinformation, malinformation is based on truth but manipulated to inflict damage.

Foreign information manipulation and interference (FIMI) refers to the activities conducted by foreign powers to distort information in order to influence political decisions, public perceptions, and undermine trust in the democratic process. The first thoroughly documented case is the Russian interference in the 2016 USA elections and was published as early as January 2017 in a report entitled Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution (Office of the Director of National Intelligence, 2017). FIMI highlights the role of state actors in information manipulation aimed at achieving geopolitical objectives and it has also been adopted in the European Union's conceptual framework through several documents, such as the Report on Stratcom activities ('2021 StratCom Activity Report - Strategic Communication Task Forces and Information Analysis Division | EEAS', 2021), and the two reports on FIMI threats published up to date (European Union External Action 2023, 2; 2024). What is worth mentioning is that the activities falling under FIMI are mostly non-illegal. The 1st Report on FIMI threats defines FIMI as "a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory" (European Union External Action, 2023, 4).

Understanding the nuanced distinctions between disinformation, misinformation, malinformation, information operations, and foreign information manipulation and interference is crucial for developing effective strategies to counter these threats. The definitions provided by the EU, NATO, or the Council of Europe offer a comprehensive framework for analysing the multifaceted nature of information manipulation. Addressing the challenges posed by these activities requires a multidimensional approach, encompassing regulatory, technological, and educational measures, as well as international cooperation.

II. Strengthening Democratic Resilience in the Euro-Atlantic space: Where to start

Democratic resilience, understood as the capacity of democratic institutions and societies to withstand and adapt to threats, both external and internal, without compromising democratic principles and processes has increasingly been at the forefront of the Euro-Atlantic community's agenda during the past decade. This chapter examines the most relevant international initiatives to bolster democratic resilience, exploring the measures implemented and the key documents that outline these strategies. Through an analysis of policy directives, summit communiqués, and strategic concepts, we delineate the alliance's approach to safeguarding democracy within its purview.

II.1. The European Union

In response to the evolving challenges facing democratic institutions and processes within its member states, the European Union (EU) has undertaken significant measures to bolster democratic resilience. These efforts aim to enhance the integrity of electoral systems, protect against disinformation, and ensure the rule of law, among other objectives. This section explores the key measures implemented by the EU to improve democratic resilience, focusing on the foundational documents that outline these initiatives. Through an analysis of policy documents, directives, and strategic frameworks, we identify the core strategies employed by the EU to safeguard democracy within its jurisdiction.

■ Action Plan Against Disinformation

The EU's Action Plan Against Disinformation (European Commission 2018) represents a critical effort to safeguard democracy against the pervasive threat of false information. This plan outlines measures for improving the detection of disinformation, strengthening coordinated responses among EU institutions and member states, and increasing societal resilience through media literacy and public awareness campaigns. It reflects the EU's proactive approach to countering disinformation and promoting informed public discourse.

■ The European Democracy Action Plan

One of the cornerstone documents addressing democratic resilience within the EU is the European Democracy Action Plan (EDAP). Announced in 2020, the EDAP outlines a comprehensive strategy to protect elections, tackle disinformation, and ensure the integrity of the democratic process (European Commission 2020). The plan emphasizes the importance of transparency in political advertising, the enhancement of media freedom, and the support of quality journalism. It proposes legislative and non-legislative measures to achieve these goals, underscoring the EU's commitment to upholding democratic standards.

■ The Digital Services Act and the Digital Markets Act

In the digital realm, the EU has introduced the Digital Services Act (DSA) and the Digital Markets Act (DMA) to regulate online platforms and protect citizens from disinformation and online harm (*Digital Services Act, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act)* 2022; *Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC* 2020). These legislative measures aim to create a safer digital space, ensuring transparency, accountability, and fairness in the operation of digital services. By addressing the challenges posed by the digital transformation, the DSA and DMA contribute to the resilience of democratic societies against misinformation and other online threats. Having entered into force on the 17th of February 2024, the DSA's key provisions include:

- **transparency requirements:** the DSA mandates greater transparency from online platforms regarding their content moderation practices, algorithms for content recommendation, and advertising systems. It requires platforms to explain how these systems work in a way that is understandable to the average user.
- **accountability measures:** online platforms, especially very large ones, are required to undergo independent audits to assess compliance with the DSA's obligations. This includes assessing risks to societal harms and the effectiveness of their systems to mitigate these risks.
- **protection against illegal content:** the DSA sets out clear obligations for the removal of illegal content while safeguarding users' rights, including the

establishment of an effective mechanism for users to report such content and for platforms to cooperate with national authorities.

- **empowerment of users:** users are given more control over what they see online, including options to opt-out of algorithmic recommendations and easier ways to report harmful content.
- **advertiser and publisher transparency:** there are specific provisions to ensure transparency in online advertising, requiring platforms to disclose why users are seeing certain ads and who is paying for those ads.

Penalties for violations under the DSA include fines which can reach 6 percent of annual revenue for very large online platforms (VLOPs), which refers to online platforms or search engines with over 45 million users in the European Union. In very concrete terms, this would amount to financial costs of roughly $11 billion for Google, for instance, or $7 billion for Meta, both of which lobbied hard against aspects of the act.

■ The FIMI Reports – Building Framework for Networked Defence

As a complimentary approach, the EU set out to build a framework that would allow it and Member States, individually, to counter foreign malign interference into democratic processes. The FIMI reports (European Union External Action 2023, 2; 2024) propose a framework to address and mitigate the risks of foreign interference and information manipulation that threaten our democracies, security, and societal cohesion, by:

- **enhancing detection and analysis:** the framework suggests improving capabilities to detect, analyse, and understand foreign interference and information manipulation campaigns, using both open-source intelligence and classified information.
- **strengthening collaboration:** it emphasizes the importance of collaboration between EU institutions, member states, and private sector actors (such as social media platforms) to share information and best practices.
- **increasing public awareness and resilience:** proposals to boost public awareness about the risks of information manipulation and strategies to enhance societal resilience are central. This includes education campaigns and the promotion of media literacy among the public.
- **regulatory and non-regulatory measures:** the framework calls for a mix of regulatory measures, such as the DSA, and non-regulatory initiatives to tackle the multifaceted challenges posed by information manipulation.
- **international cooperation:** recognizing the global nature of the challenge, the FIMI reports advocate for stronger international partnerships to counter foreign interference and promote democratic values.

II.2. NATO

The North Atlantic Treaty Organization (NATO), as a political and military alliance, has increasingly recognized the importance of democratic resilience among its member states in facing contemporary security challenges.

■ The NATO 2030 Initiative

A pivotal document in understanding NATO's commitment to democratic resilience is the "NATO 2030" initiative. Launched to ensure the alliance remains robust in a rapidly changing global security environment, NATO 2030 emphasizes the importance of political cohesion and democratic values as foundational to collective defence (Reflection Group Appointed by the Secretary General 2020). Among its proposals, the initiative calls for strengthening the political dimension of NATO, ensuring that democratic governance and resilience are central to the alliance's strategic considerations.

■ The Brussels Summit Communiqué

The Brussels Summit Communiqué of 2021 further articulates NATO's measures to improve democratic resilience. This document reiterates the alliance's dedication to the principles of democracy, individual liberty, and the rule of law. It outlines commitments to enhance consultations and coordination among member states, bolster civil preparedness, and support efforts to counter hybrid and cyber threats, which are increasingly seen as challenges to democratic institutions (NATO 2023b). The communiqué underscores the interconnectedness of security and democracy, highlighting efforts to defend against disinformation and interference in democratic processes.

NATO's and the EU's measures to improve democratic resilience are grounded in a comprehensive strategy that addresses electoral integrity, the rule of law, digital regulation, and the fight against disinformation. The foundational documents discussed in this chapter – ranging from NATO's 2030 Initiative, the European Democracy Action Plan to the Digital Services Act and the Action Plan Against Disinformation – highlight the two organisations' multifaceted approach to strengthening democracy. Through these initiatives, NATO, and, most of all, the EU demonstrate their commitment to protecting democratic values and ensuring the resilience of its democratic institutions against contemporary challenges.

III. Current challenges in bolstering democratic and societal resilience

Despite the progress that has been registered towards enhancing societal resilience and safeguarding democracies in the European landscape, neither the DSA, nor the conceptual framework proposed by the two Reports on Foreign Information Manipulation and Interference Threats are without limitations, at least for the time being. The shortcomings of the current frameworks curating the information space range from conceptual ambiguity, limited legislative frameworks and reduced agility in amending them at national levels, lack of capacity-building mechanisms to scarceness of implementation tools.

■ **Limitations of the Digital Services Act (DSA)**

A short overview of issues impending on DSA swift implementation include the need to further clarify scope and scalability, definition of illegal content, as well as balance between regulatory measures and freedom of expression.

The DSA is designed to apply uniformly across all EU member states, but the diversity in digital infrastructure, legal frameworks, and enforcement capabilities can lead to disparities in application and effectiveness. For instance, smaller member states may lack the resources and technical expertise needed to enforce the DSA's provisions effectively, leading to a scalability issue. Furthermore, challenges of regulating online content extend to the implications for smaller platforms, which often lack the resources to comply with stringent content moderation requirements. This situation is exacerbated by regulations like the EU's terrorist content regulation ('Online Regulation of Terrorist and Harmful Content' 2021), which demands rapid response times for content removal that smaller platforms staffed minimally cannot feasibly meet. The focus on larger platforms in drafting such laws overlooks the capacity constraints of smaller platforms and the diverse ways terrorists utilize online platforms, posing significant risks to the efficiency of global regulatory approaches.

Challenges also remain regarding a unitary understanding of what constitutes "illegal content". According to each Member State's peculiarity, the meaning of the notion can vary significantly across member states due to differences in national laws. This ambiguity complicates the enforcement of DSA provisions, as platforms may struggle to navigate the legal landscape and ensure compliance across all jurisdictions.

What is more, the DSA aims to regulate platforms without impinging on freedom of expression. However, the act's requirements, such as content moderation and transparency, place a heavy burden on platforms, potentially leading to over-censorship or, conversely, inadequate action against harmful content.

■ Limitations of the FIMI Reports

In an attempt to operationalise existing frameworks and facilitate a common approach, the two FIMI reports published up to date by the EEAS (European Union External Action 2023, 2; 2024) are still a long way from being implemented. Some of the obstacles that the EU and Member States will have to overcome are ascribed to coordination and consistency, measuring effectiveness, global reach vs. sovereign jurisdiction.

Firstly, the FIMI reports emphasize the need for coordination among EU institutions, member states, and private entities. However, achieving this level of coordination is challenging, especially when dealing with divergent national priorities and varying levels of commitment to the frameworks' goals.

Secondly, the reports propose measures to detect and counter foreign information manipulation, but establishing clear metrics for assessing the effectiveness of these measures is difficult. This lack of clear evaluation criteria makes it challenging to gauge the success of the FIMI initiatives and to justify the allocation of resources.

Thirdly, the FIMI reports call for international cooperation to combat information manipulation, which inherently crosses borders. However, the EU's ability to influence or control actions by entities outside its jurisdiction is limited, raising questions about the global efficacy of the FIMI strategies.

Conclusions

To sum up, the present paper offers an overview of the conceptual framework in the field of disinformation, as well as the main measures to be adopted in order to better manage the threats disinformation poses to democratic societies. The conclusion we reach is that despite the progress made to tackle information manipulation aimed at undermining democracy, the danger to our rights and freedoms is far from being removed. When it comes to frameworks devised to bolster resilience of democracies to information manipulation, implementation challenges across EU Member States revolve around: varied national capacities, legal and regulatory hurdles, technical and operational issues.

Not surprisingly, EU member states have shown diverse capacities in implementing the DSA and FIMI recommendations. For example, France (‘The French DSA’ 2022) and Germany (‘The DSA Proposal and Germany - DSA Observatory’ 2021) have taken proactive steps by incorporating DSA-like requirements into national law ahead of the EU-wide implementation. In contrast, other states, such as Romania, face significant challenges in terms of resources and expertise to effectively enforce these regulations.

Moreover, implementing current EU released frameworks, such as the DSA and FIMI, requires adjustments to national legal systems, which can be a slow and contentious process. For instance, the requirement for platforms to remove illegal content has raised legal challenges in Hungary (‘The DSA Proposal and Hungary - DSA Observatory’ 2022) and Poland (‘The DSA Proposal and Poland - DSA Observatory’ 2021), where concerns about freedom of speech and the potential for political manipulation of content moderation decisions have led to debates about the frameworks' compatibility with national laws.

Last, but not least, the operationalization of the DSA's transparency and accountability measures poses technical challenges. For example, the obligation for very large online platforms to conduct risk assessments and independent audits has required significant investment in new technologies and processes, which can be particularly burdensome for smaller platforms operating in multiple EU countries.

In conclusion, although consistent progress has been made during the past decade in understanding, recognising and addressing the threats associated with information manipulation, the road to democratic resilience remains laden with treacherous obstacles. In the light of our analysis, we have to recognise that our societies are yet not fully equipped, if at all, to manage disinformation and its effect on democracies all over the world.

BIBLIOGRAPHY:

1. '2021 StratCom Activity Report - Strategic Communication Task Forces and Information Analysis Division | EEAS'. 2021. 2021. https://www.eeas.europa.eu/eeas/2021-stratcom-activity-report-strategic-communication-task-forces-and-information-analysis-division_en.
2. Christiano, Tom, and Sameer Bajaj. 2022. 'Democracy'. In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Spring 2022. Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/spr2022/entries/democracy/.
3. Colomina, Carme, Héctor SÁNCHEZ Margalef, and Richard Youngs. 2021. 'The Impact of Disinformation on Democratic Processes and Human Rights in the World'.
4. Dahl, Robert A., Ian Shapiro, and David Froomkin. 2024. 'Democracy | Definition, History, Meaning, Types, Examples, & Facts | Britannica'. 19 February 2024. https://www.britannica.com/topic/democracy.
5. *Digital Services Act, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act).* 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065.
6. European Commission. 2018. *Action Plan against Disinformation*. https://doi.org/10.1093/law-oeeul/e66.013.66.
7. ———. 2020. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A790%3AFIN&qid=1607079662423.
8. European Union External Action. 2023. '1st EEAS Report on Foreign Information Manipulation and Interference Threats'. 1. https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf.
9. ———. 2024. '2nd EEAS Report on Foreign Information Manipulation and Interference Threats'. 2. https://www.eeas.europa.eu/sites/default/files/documents/2024 /EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf.
10. NATO. 2023a. 'NATO's Approach to Countering Disinformation'. NATO. 2023. https://www.nato.int/cps/en/natohq/topics_219728.htm.
11. ———. 2023b. 'Brussels Summit Declaration Issued by NATO Heads of State and Government (2018)'. NATO. 30 May 2023. https://www.nato.int/cps/en/natohq/official_texts_156624.htm.
12. Office of the Director of National Intelligence. 2017. 'Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attributio'. https://www.dni.gov/files/documents/ICA_2017_01.pdf.
13. 'Online Regulation of Terrorist and Harmful Content'. 2021. Default. 14 October 2021. https://www.lawfaremedia.org/article/online-regulation-terrorist-and-harmful-content.
14. Reflection Group Appointed by the Secretary General. 2020. 'NATO 2030: United for a New Era'. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

15. *Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC*. 2020. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN.
16. 'The DSA Proposal and Germany - DSA Observatory'. 2021. 12 November 2021. https://dsa-observatory.eu/2021/11/12/the-dsa-proposal-and-germany/.
17. 'The DSA Proposal and Hungary - DSA Observatory'. 2022. 11 March 2022. https://dsa-observatory.eu/2022/03/11/the-dsa-proposal-and-hungary/.
18. 'The DSA Proposal and Poland - DSA Observatory'. 2021. 22 October 2021. https://dsa-observatory.eu/2021/10/22/the-dsa-proposal-and-poland/.
19. 'The French DSA'. 2022. Lighthouse Europe. 2 March 2022. https://www.lighthouseeurope.com/the-french-dsa.
20. Wardle, Claire, and Hossein Derakhshan. 2017. 'INFORMATION DISORDER: Toward an Interdisciplinary Framework for Research and Policy Making'. *Council of Europe Publishing*, September.

1053477-3045-1396-24-10

ADVANCES IN TECHNOLOGY AND THEIR IMPACT ON MILITARY RESILIENCE – RESPONSE PLANNING A STUDY IN THE CONTEXT OF NATO'S LAYERED RESILIENCE CONCEPT

Carola FREY, PhD. candidate
Researcher, PhD. candidate at National School of Political Science and Public Administration, and analyst at Euro-Atlantic Resilience Centre, Strategic Analysis and Cooperation Department, Bucharest, Romania
E-mail: carola.frey@e-arc.ro

***Abstract**: NATO's Allied Command Transformation is developing the Layered Resilience Concept, Romania being responsible for the response planning thematic working group. This study investigates how artificial intelligence will impact military resilience, especially in the field of response planning. It highlights AI's role in accelerating decision-making and enhancing defense strategy across scenarios. Emphasizing technological advancements' contribution to military and civilian resilience, it underscores the importance of civil-military interconnectivity. Technological strength, primarily developed by the private sector, not only boosts military flexibility but also, through collaboration, enhances societal resilience and deterrence against threats and uncertainties.*

***Keywords:** military resilience, response planning, artificial intelligence, civilian resilience, layered resilience, crisis management*

Preliminary considerations

The present research makes use of a quantitative methodological framework, engaging in an analysis of documents and official communiques, alongside insights derived from thematic seminars and discussions organized by the Euro-Atlantic Resilience Centre from 2022 to the present. The objective is to examine the impact of technologies on resilience broadly, with a particular emphasis on military resilience within the realm of response planning, from a NATO perspective. The primary method of data collection of this research is the analysis of relevant documents. This includes official NATO publications, strategic planning documents from Allied Command Transformation and NATO's Strategic Warfare Development Command, policy papers, and academic literature related to military resilience and emerging technologies. The documents selected for analysis span a comprehensive range of sources to ensure a broad understanding of how artificial intelligence influences military operations and planning.

In addition to document analysis, this study incorporates findings and insights gained from thematic seminars and discussions. During 2022 and 2023, the Euro-Atlantic Resilience Centre organized a series of seminars and workshops dedicated to exploring themes of resilience and military resilience. These events, focused also around the integration and impact of technologies. They provided a platform for engaging with experts, practitioners, and policymakers, facilitating an understanding of the practical implications of technological advancements in the military sphere. Information gathered from these seminars, including presentations, discussions, and workshop outcomes, will be included to enrich the study's findings.

The primary objective of this paper is to analyse the impact of artificial intelligence on military resilience, with a specific focus on response planning. It aims to assess how these elements collectively enhance the preparedness and adaptive capacity of military and civilian sectors in the face of contemporary security challenges. Among the subsidiary goals, an evaluation will be conducted on how artificial intelligence technologies hasten the analysis and decision-making processes within the scope of response planning for a range of scenarios. This evaluation will encompass the examination of AI's role in enhancing strategic foresight, increasing operational efficiency, and boosting tactical agility within military operations.

Thus, this study contributes to the understanding and development of NATO's Layered Resilience Concept, focusing especially on the thematic area of response planning. However, it acknowledges the interconnectedness of all thematic areas within this framework (logistics, command and control, transportation, etc.), recognizing that technology plays a central role across all areas. The findings are expected to provide several perspectives on enhancing the adaptive capacity and preparedness of the Alliance in the face of evolving security challenges.

1. Technological advancements and NATO's need for an appropriate strategic perspective: a short overview

The international arena is what it has always been: a multifaceted reality in which nations strive to either maintain their security or assert their dominance. Technology has been, and continues to be, a critical factor in their strategic planning[1]. It has always been a fundamental component in foreshadowing new eras of military strategy, where conventional measures of power, such as the size of armed forces and their firepower, are progressively enhanced or surpassed by technological innovations. This evolution in strategic studies is best illustrated by technological milestones, ranging from Napoleon's mass conscription, which revolutionized the concept of national armies, to the development of armored and mechanized warfare, including the sophisticated military technologies of today (Mahnken and Maiolo 2008).

Although the fundamental nature of warfare remains unchanged, advanced technology will greatly expand and enhance the capabilities of military operations. This is particularly true of contemporary technologies and their applications, such as the use of drones for surveillance and targeted strikes, cyber warfare capabilities to disrupt enemy communications and infrastructure, artificial intelligence in decision-making, and augmented reality systems for training and battlefield simulation. These innovations are changing the strategic and tactical landscape of military engagement.

The NATO 2022 Strategic Concept articulates a dual strategy emphasizing both the enhancement of individual and collective resilience and the attainment of a technological advantage (North Atlantic Treaty Organization 2022, p. 3). This comprehensive approach acknowledges the dual nature of new and disruptive technologies, which present both significant opportunities and challenges. These technologies are transforming the landscape of conflict, becoming increasingly vital in the realm of strategic competition, and serving as focal points of international rivalry. In this evolving context, technological superiority is becoming a critical determinant of military success, underscoring the narrative that innovation is paramount (North Atlantic Treaty Organization 2022, p. 5). In response to these dynamics, NATO commits to accelerating its digital transformation efforts, aligning its command structure with the

[1] The statement draws its essence from the realist theory within international relations. Realism, as a theoretical framework, posits that states are primarily concerned with their security and position within the international system. This perspective views the quest for power and survival as the central drivers of state behavior in an anarchic international arena. Technology, from this standpoint, is integral to enhancing a state's military capabilities and securing its national interests against potential adversaries.

demands of the information age, and bolstering its cyber defenses, as well as its networks and infrastructure. This involves a proactive stance on innovation and a commitment to increasing investments in emerging and disruptive technologies. Such a strategy is essential for maintaining interoperability and preserving the alliance's military advantage (North Atlantic Treaty Organization 2022, p. 8).

Furthermore, NATO's approach includes a collaborative effort to embrace and incorporate new technologies effectively. This entails working in concert with the private sector to leverage innovation, safeguarding the alliance's innovation ecosystems, and influencing the development of international standards. Importantly, NATO emphasizes the importance of adhering to principles of responsible technology use that mirror its commitment to democratic values and human rights. This reflects a broader understanding that the key to maintaining a technological advantage lies not solely within the confines of traditional defense research and development but increasingly through partnerships with the private sector and start-ups that are at the forefront of technological innovation (Euro-Atlantic Resilience Centre 2022).

Even before the Strategic Concept of 2022 was made available to the public and outlined, the groundwork for fostering transatlantic cooperation in critical technologies was laid at the 2021 NATO Summit in Brussels. During this summit, Allied leaders came together to launch the Defence Innovation Accelerator for the North Atlantic (DIANA). This initiative was born out of a shared vision to promote interoperability among Allied forces and to bridge the gap between military needs and civilian innovation. By engaging with academia and the private sector, DIANA aimed to leverage the vast potential of emerging and disruptive technologies. The commitment to this vision was further solidified at the 2022 NATO Summit in Madrid, where all Allied Leaders endorsed DIANA's charter and announced the establishment of its initial footprint, including test centers and accelerator sites (North Atlantic Treaty Organization, DIANA, 2023).

DIANA's mission is to maintain and enhance NATO's competitive edge in collective defence and security by harnessing the opportunities presented by technologies: "*big data, artificial intelligence (AI), autonomy, quantum, biotechnologies and human enhancement, energy and propulsion, novel materials and advanced manufacturing and space – specifically where they are dual-use (civilian and defence) and deep tech in nature, and where they can be used to solve challenging defence and security problems*" (North Atlantic Treaty Organization, DIANA, 2023). The initiative underscores the Alliance's commitment to adapting and thriving in an era where emerging and disruptive technologies are reshaping the landscape of peace, crisis, and conflict ((North Atlantic Treaty Organization, DIANA, 2023).

In 2021, alongside the development of DIANA, NATO approved the NATO Warfighting Capstone Concept (NWCC). This strategic framework is aimed at enhancing the Alliance's deterrence and defense capabilities, providing a roadmap for sustaining and augmenting NATO's critical military edge. By focusing on adapting the military power continuum until 2040, the NWCC specifically addresses emerging challenges in great power dynamics (North Atlantic Treaty Organization, NWCC, 2021). The document places significant emphasis on bolstering the Military Instrument of Power (MIoP) as a key strategy for enhancing an Alliance's ability to respond to strategic surprises and confrontations with adversaries through Layered Resilience. It highlights the importance of adopting a comprehensive resilience strategy that integrates both military and civilian aspects. This integrated approach is crucial not only for remaining prepared for unforeseen incidents but also for maintaining enduring resilience and superiority against potential foes.

By adopting the "2021 Strengthened Resilience Commitment", Allies have underscored the critical importance of both national and collective resilience as foundational to effective deterrence and defense. This commitment, rooted in Article 3 of the Washington Treaty, highlights resilience as both an individual national duty and a shared Alliance obligation. A successful deterrence and defense strategy hinges on a robust Military Instrument of Power (MIoP), capable of safeguarding Alliance territories and populations against all threats. This involves ensuring readiness, durability, and adaptability to strategic upheavals, thereby enhancing the Alliance's overall resilience. This resilience is instrumental in absorbing shocks and maintaining critical services and government functions, crucial for military operations across peace, crisis, and conflict scenarios. The concept of Layered Resilience, evolving in alignment with NATO's broader resilience efforts and the outcomes of the 2021 Summit, integrates military and civil resilience, emphasizing their interdependence and the need for a holistic approach to address and mitigate critical vulnerabilities and risks within the Alliance (North Atlantic Treaty Organization, LRC, 2021).

Military resilience, while a subject of extensive debate and lacking a clear definition, with scholars and practitioners still discussing its precise nature, undeniably overlaps with, and relies on civilian resilience. This includes the continuity of government, infrastructure, societal resilience, among others. Similarly, technology's role is significant and parallels its impact on civilian sectors. In fact, the civilian sector now spearheads certain technologies critical to the military, in areas such as cybersecurity, encryption, UAVs, space technologies (just to name a few). Additionally, the context of peace versus conflict introduces a crucial distinction: peace brings stability and calm, whereas conflict alters the perception and progression of time, demonstrating a fundamentally different dynamic.

An October 2022 NATO document describes military resilience as "*A resilient NATO Military Instrument of Power (MIoP) or simply military resilience, supports the deterrence and defence of the Alliance through its ability to anticipate, prepare for, and adapt to threats and hazards and, to withstand, respond and recover rapidly from strategic shocks*" (North Atlantic Treaty Organization, ACT, 2022). Seen through this lens, military resilience is essentially about the proactive and reactive capabilities of NATO forces. Proactively, it involves being vigilant and prepared for potential threats, which requires constant analysis and adaptation to evolving global security dynamics. Reactively, it encompasses the ability to quickly recover from unforeseen challenges, ensuring that the Alliance remains robust and operational even after facing severe disruptions. This dual focus not only aims to prevent conflict through a show of strength (deterrence) but also ensures that NATO can effectively defend its members should deterrence fail. It underscores the importance of flexibility, preparedness, and rapid response in maintaining security and stability in the face of complex, modern threats.

Technology significantly enhances military resilience by playing a role in various aspects of defense readiness. Technological advancements in surveillance and communications systems are key to early threat detection. Likewise, innovations in training, equipment, and logistics bolster preparedness and flexibility. Technology's importance extends to post-conflict recovery, ensuring rapid return to operational status. By embracing state-of-the-art technologies, NATO secures a strategic edge, effectively countering threats and underscoring its dedication to advancing military capabilities to meet contemporary challenges.

2. The role of AI in military resilience and response planning

The integration of artificial intelligence in the military domain represents one of the most explicit shifts in how defense strategies are formulated, executed and how they evolved in time.

NATO's acknowledgment of AI as an Emerging and Disruptive Technology (EDT), along with the creation of a dedicated strategy (North Atlantic Treaty Organization, AI, 2021), highlights its capacity to greatly improve military capabilities, procedures, and operational efficiency. This recognition goes beyond merely equipping Allies with advanced technology for defense purposes - it is primarily about maintaining strategic superiority and ensuring security in an increasingly complex architecture. Apart from this, it is also about addressing the necessity to "*confront today's and tomorrow's critical challenges*" (North Atlantic Treaty Organization, ACT, 2019), leveraging AI and dual-use technologies to provide innovative solutions that enhance decision-making and operational capabilities in complex scenarios.

AI in the military field involves the use of algorithms, machine learning, and other computational methods to process and interpret data at speeds and scales that are outside human capabilities, enabling the identification of trends, patterns, and potential threats that may not be immediately apparent (ADF Solutions 2023). These technologies can automate routine tasks, provide actionable insights in real time, and support complex decision-making processes (Sauer 2022, pp. 28-30). Frank Sauer argues about AI's potential in improving decision-making, sensing, and acting in military contexts, while also acknowledging the risks and the overestimation of AI's reliability and effectiveness in these settings. AI and Machine Learning's (ML) misunderstood nature, marked by their limitations to specific tasks, poses significant challenges, emphasizing the need for a balanced understanding of their capabilities and limitations in military applications.

The challenges associated with achieving resilience in AI-enabled military systems imply dealing with the inherent "brittleness" of ML-based systems, which can fail unexpectedly when faced with scenarios slightly different from their training data (especially if the data is nor properly curated/sanitized), and the "opacity" of AI decisions, which makes it difficult to predict or understand AI actions in complex military environments.

Expanding upon the integration of AI in enhancing military resilience and response planning, it is crucial to consider the transformative impact it has on the strategic depth and adaptability of military operations. The use of AI and ML in this context, if applied correspondingly, transcends conventional defense mechanisms, offering a multifaceted platform for intelligence gathering, risk assessment, and strategic foresight (Riddell et al. 2019). This capability is invaluable in crafting preemptive strategies and response plans that are both precise and contextually relevant. AI's contribution to military resilience is evident in its ability to optimize resource management and operational readiness. Through simulation and modeling techniques, AI can forecast logistical challenges and suggest efficient solutions, ensuring that military forces are better prepared and equipped to respond to crises. Additionally, AI-enabled communication and coordination tools enhance the interoperability of forces, facilitating seamless collaboration among allies and improving the collective response capability of the Alliance.

However, the integration of AI into military resilience and response planning also necessitates a robust framework for ethical considerations, transparency, and accountability. As AI systems take on more critical roles in decision-making processes, establishing clear guidelines and oversight mechanisms becomes imperative to prevent misuse and ensure that actions taken follow international law and humanitarian principles (Gomez 2019, pp. 8-9). This balanced approach to incorporating AI reflects a forward-thinking mindset that prioritizes both technological advancement and the ethical implications of its application in military contexts, thereby reinforcing the Alliance's commitment to safeguarding peace and security in an increasingly complex and interconnected world.

An illustrative example of how AI can serve as a useful tool for response planning within the concept of layered resilience, particularly in managing a multilevel crisis such as a pandemic, spans across the entire spectrum of NATO, regional, national, and cross-Instrument of Power (IoP) levels. This integrated approach to contingency planning leverages AI's capabilities to enhance situational awareness, predictive analytics, and decision support systems, thereby facilitating a coordinated and agile response to crises.

At the NATO level, AI can analyze vast amounts of data from global health organizations and intelligence sources to identify potential pandemic threats before they become widespread. By employing machine learning algorithms to detect patterns and anomalies in disease outbreak data, AI systems can forecast the spread of infections, enabling NATO to prepare and deploy resources more effectively.

Regionally, AI can support the coordination of cross-border public health responses. Through the analysis of travel and communication data, AI can help predict the path of disease transmission between countries, allowing for the implementation of targeted travel restrictions or the provision of medical support to areas predicted to be most affected.

Nationally, governments can use AI to optimize the allocation of medical resources, including hospital beds, ventilators, and vaccines. Predictive models can forecast demand for medical services, guiding the distribution of resources to areas with the greatest need (United Nations Academic Impact). Additionally, AI-powered chatbots and information platforms can provide the public with real-time, accurate information about the pandemic, improving community preparedness and compliance with public health measures.

Cross-IoP, AI can facilitate the integration of military, civil, and private sector efforts in pandemic planning and response. For example, AI can enhance logistic networks, ensuring the efficient distribution of medical supplies and vaccines by analyzing supply chain vulnerabilities and optimizing routes. Furthermore, AI can support the development of pandemic simulations and exercises, enabling decision-makers to test and refine their strategies in a virtual, and therefore safe environment, improving interoperability and coordination across different sectors and levels of government (Vila Maior and Camisão 2022, pp. 29-56).

This comprehensive, AI-enabled approach to layered resilience and contingency planning exemplifies how technology can significantly enhance the ability of NATO, regional alliances, national governments, and cross-sectoral partnerships to anticipate, prepare for, adapt to, and recover from a pandemic or similar multilevel crisis. Through the strategic application of AI, stakeholders can achieve a more cohesive, responsive, and effective management of complex emergencies, thereby safeguarding public health and maintaining security and stability across diverse communities.

While AI offers significant opportunities, there are several challenges and limitations to its deployment in such contexts. These challenges span technical, ethical, legal, and operational domains, underscoring the need for a cautious and well-regulated approach to AI integration in military and civil defense strategies. AI systems rely heavily on the availability of high-quality, comprehensive data. In the context of a global crisis, obtaining real-time, accurate data across different regions and jurisdictions can be challenging due to disparities in data collection methods, privacy laws, and the willingness of entities to share information. Inconsistent or biased data can lead to inaccurate predictions and analyses, potentially compromising response efforts.

AI algorithms can inherit or amplify biases present in their training data, leading to decisions that may disproportionately affect certain populations or regions. Ensuring fairness and equity in AI-driven decisions, such as resource allocation or prioritization of response efforts, is a significant challenge that requires ongoing attention and mitigation strategies.

Achieving seamless communication and operation of AI systems across NATO remains an ongoing objective. However, differences in technological infrastructure, data formats, and operational protocols can hinder this integration, limiting the effectiveness of a coordinated response. Moreover, AI systems are susceptible to cyber-attacks, including data breaches, denial of service attacks, and adversarial attacks designed to manipulate AI decision-making. Protecting these systems from cyber threats is critical to ensuring that they function as intended, especially in high-stakes scenarios like pandemic or even conflict response planning.

The use of AI in crisis response planning raises complex ethical and legal questions, particularly regarding accountability, consent, and privacy. Determining who is responsible for AI-driven decisions, how to obtain consent for data use in emergency situations, and how to protect individual privacy are challenges that require careful consideration and regulation. Overreliance on AI can lead to a degradation of human expertise and judgement, especially if AI recommendations are followed without any shroud of critical assessment. Ensuring that human decision-makers remain in the loop and that AI serves as a support tool, rather than a replacement for human judgement, is essential for maintaining a balanced approach to crisis management.

In the face of various crises, such as natural disasters including earthquakes and floods, the flexibility and potential significance of AI and ML technologies in a wide range of emergency situations become increasingly apparent (Munno, Proto, & Trancu 2023).

These natural catastrophes, unlike pandemics, often strike with little to no warning, demanding rapid, effective, and well-coordinated response efforts to mitigate loss of life, infrastructure damage, and long-term societal impacts. The integration of AI into military and civil strategies for handling such crises can substantially enhance the effectiveness and efficiency of response operations.

For earthquakes, AI has a role to play in early warning systems, where even a few seconds of advance notice can save lives by allowing people to move to safer locations and automatically shutting down critical infrastructure to prevent further damage. AI algorithms can analyze seismic data in real time to detect unusual patterns that may indicate an imminent earthquake, providing valuable time for response measures. Post-earthquake, AI tools can assist in damage assessment, analyzing satellite and drone imagery to identify areas of destruction and prioritize search and rescue operations. This rapid assessment capability ensures that resources are directed where they are most needed in the crucial hours following a disaster.

In the context of flood management, AI and ML technologies offer significant advancements in predictive modeling and risk assessment. By processing vast amounts of meteorological data, AI systems can predict flood events with greater accuracy, forecasting the timing, intensity, and potential impact areas of flooding. This information is critical for early warning systems, enabling timely evacuation orders and the preparation of flood defenses. Furthermore, AI can support the management of water resources, such as dams and levees, optimizing their operation to mitigate flood risks. After a flood, AI-powered analysis of aerial imagery can quickly assess damage to infrastructure and agricultural lands, facilitating an organized and effective recovery process.

The integration of AI into military resilience and crisis management for earthquakes and floods also underscores the need for robust, multi-layered communication networks. AI-enabled communication systems can ensure uninterrupted information flow even in the aftermath of these disasters, maintaining coordination among military units, emergency services, and humanitarian organizations. This seamless communication is crucial for coordinating rescue efforts, distributing aid, and providing medical assistance to affected populations (Guha, Jana, & Sanyal 2022).

Moreover, AI can enhance the strategic planning and execution of military logistics in the wake of natural disasters. By predicting the impact on transportation networks and supply chains, AI systems can identify alternative routes for the delivery of relief supplies and equipment, ensuring that aid timely reaches those in need despite damaged infrastructure. This logistic support extends to planning for temporary shelters, medical facilities, and the distribution of food and water, all of which are critical components of an effective disaster response (Latvakoski, Öörni, Lusikka, & Keränen 2022).

However, as with pandemics, the deployment of AI in response to earthquakes and floods presents unique challenges and considerations. The accuracy of AI predictions and analyses depends heavily on the quality and quantity of data available, which can be limited or difficult to collect in real-time during natural disasters. Moreover, the ethical, legal, and operational issues highlighted in the context of pandemic response, such as data privacy, bias in AI algorithms, and the need for human oversight, are equally pertinent in the management of earthquakes and floods (Ghaffarian, Taghikhah, & Maier 2023).

To overcome these challenges, a collaborative approach that involves the military, government agencies, international organizations, and the private sector is essential. Such collaboration, if based on a shared understanding of common problems and openness, can facilitate the sharing of data and expertise, enhance the interoperability of AI systems, and ensure that ethical and legal standards are upheld in the deployment of AI for disaster response. Additionally, continuous investment in AI research and development, along with training for military and civilian personnel in the use of AI tools, will be key to maximizing the potential of AI in enhancing resilience and response capabilities for a wide range of crises, including but not limited to pandemics, earthquakes, and floods.

3. Enhancing NATO’s response planning through AI-driven resilience mapping

To bolster resilience and enhance response planning, NATO, leveraging AI technology enriched with extensive data, can precisely map out the interconnectedness and frailties within military and civilian frameworks, guided by the seven baseline requirements. This strategic approach allows for the identification of critical “breaking points” and gaps between these frameworks, facilitating the development of a comprehensive matrix that elucidates the dynamics of interactions and potential vulnerabilities. Understanding these relationships and how they could be exploited is key to fortifying NATO’s preparedness and defense mechanisms against diverse threats and challenges.

This methodology not only strengthens resilience but also ensures a more informed and agile response strategy in the face of crises. It identifies training areas for future improvement, ensuring that preparedness evolves with emerging challenges. By pinpointing where enhancements are needed, it allows for targeted training initiatives, strengthening both immediate responses and long-term resilience strategies. This forward-looking approach ensures that responses to future crises are not only swift but also grounded in a deep understanding of past incidents and current capabilities, thereby enhancing overall crisis management effectiveness.

Experience has shown that a crisis affecting one sector, such as transport, can have far-reaching effects on other sectors (energy or society), leading to a multi-level crisis in which the initial impact is amplified by interconnected systems. This cascading effect underscores the need for a holistic and integrated approach to crisis management and planning. Understanding these complex interdependencies allows for more effective mitigation strategies, ensuring that responses are not only rapid but also targeted across the multiple levels affected, thereby minimizing the potential for amplification of the initial crisis.

Thus, if used and implemented effectively, AI and technology can greatly enhance the ability to identify and address these interconnected vulnerabilities before they escalate. AI systems, with their data analytics and pattern recognition capabilities, can pinpoint potential crisis points and suggest preventative measures. This enables a more proactive approach to crisis management, ensuring that responses are positive rather than reactive, thereby reducing the potential impact of such crises across multiple domains and levels.

Additionally, leveraging AI, can precisely identify where military and civilian resilience may falter, finding areas for improvement. This technology can enable in this matrix the strategic deployment of capabilities where they are most needed, ensuring efficient use of resources.

Conclusions

Advances in technology, notably artificial intelligence, have a significant impact on military resilience and response planning, offering unprecedented capabilities for early threat detection, decision-making, and operational efficiency. This research offers a snapshot into the significant role of AI, showcasing how technological advancements promote a mutual enhancement of resilience across military and civilian sectors. AI can accelerate the analysis and decision-making processes in response planning and reinforce strategic foresight and tactical agility.

The engagement with the private sector through public-private partnerships is however essential, driving technological advancements that underpin both military flexibility and societal resilience. This collaborative approach is crucial for addressing contemporary security challenges, ensuring that NATO maintains a technological edge in an increasingly complex security landscape.

Military resilience cannot be established in isolation from civilian components. The foundation of military resilience reveals vulnerabilities that necessitate collaboration with the private sector and reliance on services that extend beyond traditional military domains. It is crucial for military resilience strategies to maintain a close connection and alignment with civilian developments, especially in the context of adopting new technologies. This necessity becomes particularly evident in the integration of artificial intelligence, a field predominantly driven by the private sector. NATO's adoption of AI across various mechanisms underscores the importance of bridging military capabilities with civilian technological advancements. The symbiosis between military and civilian sectors is central in augmenting the military's resilience, making it more robust, adaptable, and proficient in assimilating state-of-the-art innovations to amplify its operational efficiency. This interconnection fosters an environment where advancements in technology, particularly in artificial intelligence, can be seamlessly integrated into military strategies. Such integration markedly boosts NATO's adaptive capacity, readiness, and overall resilience. The seamless incorporation of AI into military frameworks not only enhances strategic capabilities but also ensures that NATO remains at the forefront of technological advancements, ready to address contemporary and future security challenges.

BIBLIOGRAPHY:

1. ADF Solutions. „The Power of AI in Military Intelligence: How Machines Change the Game." ADF Solutions, March 15, 2023. https://www.adfsolutions.com/news/the-power-of-ai-in-military-intelligence-how-machines-are-changing-the-game
2. Gomez, I. „Artificial Intelligence & Machine Learning in Public Safety." European Emergency Number Association (EENA), 2019.
3. Guha, S., Jana, R. K., & Sanyal, M. K. „Artificial neural network approaches for disaster management: A literature review." *International Journal of Disaster Risk Reduction* 103276 (2022). https://doi.org/10.1016/j.ijdrr.2022.103276
4. Latvakoski, J., Öörni, R., Lusikka, T., & Keränen, J. „Evaluation of emerging technological opportunities for improving risk awareness and resilience of vulnerable people in disasters." *International Journal of Disaster Risk Reduction* 80 (2022): 103173. https://doi.org/10.1016/j.ijdrr.2022.103173
5. Mahnken, T., & Maiolo, J. A., eds. *Strategic studies: A reader*. 1st ed. Routledge, 2008.
6. Munno, C., Proto, I., & Trancu, P. „AI and Disaster Management: Potential and Applications." About Resilience. Retrieved from https://www.aboutresilience.com/ai-and-disaster-management-potential-and-applications/ (2023).
7. North Atlantic Treaty Organization. „Strategic Concept 2022." https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf (2022).

8. Euro-Atlantic Resilience Centre. *Building Hybrid Threats Resilience in the Era of AI and Disruptive Technologies.* Euro-Atlantic Resilience Forum 2022. Bucharest, 2022.
9. North Atlantic Treaty Organization. „Defence Innovation Accelerator for the North Atlantic (DIANA).” https://www.nato.int/cps/en/natohq/topics_216199.htm (2023).
10. North Atlantic Treaty Organization. „Defence Innovation Accelerator for the North Atlantic (DIANA): About DIANA.” https://www.diana.nato.int/about-diana.html (2023).
11. North Atlantic Treaty Organization. „The NATO Warfighting Capstone Concept.” https://www.act.nato.int/our-work/nato-warfighting-capstone-concept/ (2021).
12. NATO. February 6, 2022. Layered resilience concept proposal submission.
13. NATO ACT. October 4, 2022. What is Military Resilience (MR)?
14. NATO. „An Artificial Intelligence Strategy for NATO.” *NATO Review*, October 25, 2021. https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html
15. NATO ACT. „Artificial Intelligence – A Game Changer for the Military.” October 25, 2019. https://www.act.nato.int/article/artificial-intelligence-a-game-changer-for-the-military/
16. Riddell, G. A., van Delden, H., Maier, H. R., & Zecchin, A. C. „Tomorrow's disasters – Embedding foresight principles into disaster risk assessment and treatment.” *International Journal of Disaster Risk Reduction* 101437 (2019). https://doi.org/10.1016/j.ijdrr.2019.101437
17. Sauer, F. „The military rationale for AI.” In T. Reinhold & N. Schörnig (Eds.), *Armament, Arms Control and Artificial Intelligence: The Janus-faced Nature of Machine Learning in the Military Realm*. Springer Nature Switzerland, 2022.
18. United Nations Academic Impact. „Helping to Fight the COVID-19 Pandemic with Artificial Intelligence.” United Nations. https://www.un.org/en/academic-impact/helping-fight-covid-19-pandemic-artificial-intelligence

1053477-3045-1396-24-11

RUSSIAN FEDERATION IN 2024 – DIME-FIL ANALYSIS

Raluca Elena RADU
Lieutenant-commander, Master's Degree Student, Command and Staff Faculty, Navy Department, National Defense University "Carol I", Bucharest, Romania
E-mail: eralucaradu@gmail.com

Valentin-Lucian MAFTEI
Lieutenant (N), Master's Degree Student, Command and Staff Faculty, Navy Department, National Defense University "Carol I", Bucharest, Romania
E-mail: vmaftei88@gmail.com

Abstract: *The current reality, increasingly characterized by ambiguity, uncertainty, and complexity, necessitates new, deep, and comprehensive analyses, as military domain analysis alone is no longer sufficient. Therefore, there is a need to approach new tools that cover a broader spectrum, including diplomatic, informational, military, and economic domains.*

Within this endeavour, we aim to conduct an analysis of the current security environment, with a focus on the Russian Federation, from the perspective of DIME-FIL. Through this study, we seek to provide a conducive framework for forecasting the evolution of the Russian Federation in the year 2024, employing both longitudinal analysis and a cross-sectional analysis of Russia's involvement in the conflict in Ukraine. This is intended to diagnose issues and generate hypotheses regarding the future actions of the Federation.

We believe that our initiative is timely because effective anticipation of the actions of the Russian Federation in the year 2024 will enable efficient planning of forces and resources, both at the regional level and within the framework of alliances.

Keywords: *DIME-FIL, Russian Federation, Ukraine, Black Sea*

Introduction

On October 1st, 1939, Winston Churchill, during his first broadcast on BBC Home Service radio, discussed the unpredictability of Soviet action during World War II and remains memorable for his definition of Russia: "*I cannot predict the action of Russia. It is a riddle shrouded in a mystery inside an enigma, but perhaps there is a key. That key is the Russian national interest*". (*Churchill, 1939*)

In the current uncertainty and complexity of the Russian Federation's actions in Ukraine, the definition of the British leader is confirmed even in the aggression provoked two years ago.

In this endeavour, we aim to determine the strategy adopted by Russia in the war that began on February 24, 2022, by analysing both the modus operandi of this country and the responses to the following questions (JDN 1- 18, 2018):

- Where does it want to go or what is the desired end state? (END)
- How will it reach its goals or what are the ways? (WAYS)
- What resources does it have at its disposal? (MEANS)
- What are the risks and costs of this strategy? (RISKS and COSTS)

According to official statements, Russia harboured significant resentment towards independent Ukraine, viewing it as a critical part of the "Mother Russia" concept. Russian President Vladimir Putin consistently promoted the historical notion that Ukrainians and

Russians constitute "one nation." (The Associated Press, 2019)

Analysing the modus operandi of the Russian Federation, ten years ago, in 2014, its ambitions were similar and started with the illegal crossing of Ukraine's state border by Russian troops in order to occupy the Crimean Peninsula (ends). The timeline of events during that period was as follows: the occupation of the Parliament and Council of Ministers of Crimea, the organization and winning of the "referendum on the status of Crimea," the blocking of land entries and airports in the peninsula. In less than a month, the Autonomous Republic of Crimea was declared, and Sevastopol was completely occupied by Russian armed forces. Internationally, the United States and the European Union imposed the first sanctions for the occupation of Crimea, and the United Nations General Assembly adopted Resolution 68/262, emphasizing that the referendum in Crimea had no validity. Numerous confrontations, illegal referendums, casualties, and negotiations ensued for cities such as Donetsk, Kharkov, Slovyansk, Kramatorsk, Druzhkivka, Kherson, Luhansk, Mykolaiv, Odesa, which were considered by the Russian president as "*Novorossiya*." One year later, on February 21, 2015, cities and villages in the Donetsk and Luhansk regions were recognized by the Ukrainian Parliament as temporarily occupied territories. (Ralph, 2014)

The series of unconventional attacks on Ukraine continued and included the bombing of critical infrastructure in Avdiivka on 29 January 2017, the massive cyber-attack on Ukrainian companies and government agencies on 27 June 2017, and the attack on 3 Ukrainian vessels in the Kerch Strait on 25 November 2018.

Even the year 2021 was not peaceful regarding the two countries, and Russia's offensive in the near future was looming. Russia blocked part of the Black Sea and brought troops to the border with Ukraine (November 2021 - 90,000 troops), followed by the military exercise "Union Resolve 2022" in early February 2022, conducted jointly with Belarus. (Russian News Agency), 2022

The occupation of Crimea represented just one tangible manifestation of the decades-long hybrid campaign to compel Kiev to accept Moscow's dominance. However, Russia's desire for expansion did not stop there, and on February 24, 2022 (Boris, 2022), Russia launched a full-scale war against Ukraine. As the war is still ongoing, we aim to analyse Russia's strategy through the lens of various instruments of power.

The strategic means available to a state are often referred to as instruments of power: Diplomatic, Informational, Military, Economic, Financial, Intelligence, and Legal/Law Enforcement (DIME-FIL).

For a long time, the term DIME has been used to define the instruments of power of a country or alliance: Diplomatic, Informational, Military, and Economic. With the emergence of terrorist aggressions, the acronym has been expanded to encompass various types of threats during conflicts. DIME has evolved into DIME-FIL, where F represents the financial instrument, as the flows of money necessary for financing conflicts, I stands for intelligence collection or activities of intelligence services, and L represents the force of understanding and enforcement of national and international laws.

From a doctrinal point of view, at the level of the United States Air Force, "The Joint Team" has been issued, in which all the instruments of power are presented, with the aim of preventing aggression of the actors and achieving strategic level objectives. (US Air Force, 2022)

From this perspective, we observe the actions of the Russian Federation since the beginning of the aggression in 2022, using the instruments of power as criteria for analysis and aiming to make a prediction regarding its evolution in the year 2024.

1. The Diplomatic Instrument

The essence of the diplomatic instrument lies in the involvement, namely how a nation interacts with state or non-state actors, generally to ensure a form of agreement that allows conflicting parties to coexist peacefully. (JDN 1-18, 2018)

The international diplomatic reality since the beginning of the Russian Federation's aggression maintains the appearance of peaceful coexistence but acts aggressively. This is confirmed by the approximately 600 Russian diplomats expelled from Western countries, under various pretexts, both in the context of the war and accused of engaging in activities incompatible with the status of diplomats. (Russian News Agency, 2022)

However, the diplomatic relations developed by the Russian Federation are maintained within the multilateral cooperation group BRICS. BRICS is a group composed of major non-Western powers from different continents (Brazil, Russia, India, China, and South Africa), countries representing 46% of the world's population, 29% of the global GDP, and 25% of goods exports. (Marcus, 2023)

The conflict provoked by the Russian Federation in Ukraine at the beginning of 2022 was viewed differently by the partner countries in BRICS. Brazil was the only state to join the 141 nations in the UN General Assembly in March 2022 to support a resolution condemning Russia's actions, while the other states abstained. (General Assembly resolution, 2022) However, Russia maintains that its policy is supported internationally, which may be a national objective (end state).

Viewed from another perspective, over the 2 years of confrontations, the United States of America pursued three diplomatic priorities: supporting Ukraine, strengthening NATO, and attempting to avoid a war with Russia. Moreover, the pace of official visitors to the U.S. Embassy in Kiev has increased exponentially, ranging from members of Congress to the White House and cabinet officials. (Derek, 2023)

In addition to the information-sharing network of Five Eyes (a close partnership with Canada, Australia, the United Kingdom, the United States, and New Zealand), America has enhanced its information-sharing with NATO allies, France, and Germany. The challenge for American diplomats is how the United States can help Ukraine win its war while simultaneously avoiding escalation with Russia.

From a diplomatic perspective, we can conclude that although the West reacted unitedly against Russian aggression, they failed to engage players such as India or China. Many governments preferred to adopt a position of ambiguity towards Russia, and we can argue that diplomacy and diplomatic creativity will be necessary when assessing the political and economic costs of the war.

2. The Informational Instrument

Information security primarily refers to preventing leakage, distortion, and destruction of information, both within organizational domains and governments. The current conflict has demonstrated how Russia and Ukraine use social networks as means (**ways**) to present their versions of the events and to amplify contrasting news about the war, including its causes, consequences, and continuation. Government officials, individual citizens, and state agencies have turned to a variety of platforms, including Facebook, Twitter, TikTok, YouTube, and Telegram, to massively upload information. For example, in just the first week of the war, videos from a series of sources on TikTok with the tags #Russia and #Ukraine garnered 37.2 billion and 8.5 billion views, respectively**.** (Christian, 2022). Facebook and Twitter are both banned within Russia's borders, but Russian propaganda and disinformation targeting external audiences still flourish on these platforms. (John, 2023). On the other hand, YouTube and TikTok applications are still accessible to ordinary citizens, but with strong censorship.

The restrictions imposed by the government on these major social media platforms leave Telegram as the primary accessible source for both Russians and Ukrainians. Telegram is an encrypted messaging service created and owned by Russian technology billionaire Pavel Durov, which is being used in the war for everything from connecting Ukrainian refugees to safe passage opportunities to providing near real-time videos of events on the battlefield. Critically, in the fight against misinformation, Telegram does not have official policies to censor or remove content of any kind. While some channels on Telegram have been shut down, the company does not issue official statements about the reasons, and generally allows most user-posted content to circulate, regardless of its nature. This allows Telegram to serve as a largely unfiltered source of disinformation in Russia and Ukraine.

However, countries have taken action to counter the population's exposure to misinformation. For example, in the United Kingdom, a government information cell was established shortly before the invasion to support public communication efforts in debunking and countering Russian disinformation campaigns. It operates across various government ministries, producing strategic communication content to share online and providing guidance to up to 30 NATO and EU allies. (Edward, 2022)

The combat against the informational instrument of power was evident on January 23, 2024, when the United Kingdom, the United States, and Australia sanctioned Russian cyber hacker Aleksandr Gennadievich Ermakov in a coordinated action aimed at combating international cybercrime. Mr. Ermakov was a key actor in the 2022 Australia Medibank cyberattack, which exposed 9.7 million records and data of customers concerning over 480,000 health complaints leaked on the dark (Foreign Commonwealth, 2024).

Russia employs various strategies to introduce, amplify, and spread false and distorted content worldwide, using a set of state-owned mass media, websites, anonymous accounts, and other methods of propaganda dissemination that promote Kremlin's interests and undermine its opponents. Government-funded and managed websites utilize digital platforms such as YouTube, Facebook, Twitter, and TikTok to launch and promote fake news. The plethora of information available online can be processed through critical thinking mechanisms (Cioranu, 2021). We can conclude that disinformation is a quick and relatively inexpensive way to destabilize societies and set the stage for potential military actions.

3. The Military Instrument

It is represented by the use of force in an attempt to impose one country's will upon another. This may involve the application of force, the threat of force, or allowing other parties to apply force to achieve strategic goals. (JP 1, 2018). Operationally, the military operational instrument does not distinguish between the type of operation, whether it be land, air, or naval, which is why we will focus on naval warfare, as it has been defined up to this point.

In the two years of confrontations, the conflict in Ukraine has been perceived as a land war. We confirm that the naval aspects of the conflict have not received due attention, although they have altered the courses of action of the Russian Federation.

Firstly, from the beginning of the conflict, the Russian Navy sought to establish a long-term blockade against Ukraine (**means**), focusing on halting Ukraine's main grain-exporting port, Odesa (**ways**). At the onset of hostilities, the Russian Navy deployed a significant contingent of warships and missile-armed submarines to prohibit Ukrainian navigation in the Black Sea (**ends**). Both Russia and Ukraine have deployed minefields (**ways**) along the southern coast of Ukraine intending to target each other's military forces (**ends**), which has hindered the movement of both warships and commercial vessels. (Bhavya, 2022)

Secondly, the Russian Navy has supported Russian ground forces with air defence and long-range precision strikes on Ukrainian ground targets (**ways**). After the initial months of conflict, as Russian troops began to shift their strategy towards eastern Ukraine, there was an increasing need to establish an air defence system to protect Russian ammunition depots and logistical installations (**means**) against potential Ukrainian airstrikes. (Mykhaylo, 2022) Russia's submarines and warships armed with missiles provided the Russian army with additional attack capability (**ways**). While Russian forces captured Snake Island (Dobrin, 2025), a small island marking the boundaries of Ukraine's exclusive economic zone, and neutralized Ukraine's weak naval forces in the early days of the war, Russia's amphibious group was tasked with containing Ukrainian forces around Odesa and leading limited amphibious forces. However, landings in the Sea of Azov to support Russia's ground campaign (**ends**) did not take place. (Tayfun, 2022) It is relatively easy to control the sea in open seas, such as in the Mediterranean Sea, but very difficult, almost impossible, in a semi-enclosed sea like the Black Sea. (Nistor and Scipanov, 2021, 30)

The centre of gravity for the naval confrontation during this war was the sinking of the flagship vessel Moskva. The loss of one of the prestigious units of the Russian Navy, the former flagship of the Black Sea Fleet, the guided missile cruiser Moskva of the Slava class (Project 1164), during the war in Ukraine, is a symbolic event in different ways for both parties. This event sent shockwaves through Russia's political and military institutions. Shortly after the attack, the Russian fleet was relocated to the eastern port of Novorossiysk on the Black Sea (**means**).

The critical thinking that any military could develop is related to Turkey's control over the Sea of Marmara, specifically the Bosporus and Dardanelles straits. Moscow could have closed all Ukrainian ports if Turkey had not closed the Bosporus and Dardanelles straits to warships. (Heather, 2022)

Although Ukraine's success in naval warfare was attributed to its fleet of drones, the forecast for the evolution of the Russian Federation in 2024 from a military standpoint will include record increases in military spending to modernize the armed forces, new waves of mobilizations following the presidential elections, and a strategy aimed at exhausting Ukraine's forces. The new recruits will be trained to maintain technological superiority, and there will be a focus on developing capabilities in electronic warfare, unmanned aerial vehicles (UAVs), and informational warfare.

4. The Economic Instrument

The economic power instrument is utilized at the political level to influence the behaviour of another state, such as through trade agreements, tariffs, embargoes, or economic sanctions. The strategic vision of economic sanctions against the Russian Federation must be assimilated with a military strategy. Thus, the ends, ways, and means have been fundamental elements of the economic strategy.

When Russia began its large-scale invasion of Ukraine on February 24, 2022, the United States, the European Union, several other G7 economies, and their allies responded with an unprecedented package of economic sanctions that were continuously modified in the following months. (Richard, 2023)

An eloquent example of the firm stance of international forces is the blocking of Russian oil tanker shipments, which had a different price compared to the ceiling set by the G7 Oil Price Cap Coalition (at $60 per barrel). (European Commission guidelines, 2023) . This action underscores the commitment of G7 members to responsibly reduce the revenues from oil that the Russian government can use to finance its brutal invasion of Ukraine.

Additionally, the sanctions have affected the supply chains of the Russian Federation in the military-industrial complex. Throughout the conflict, Russia has continued to exploit economic relations with the People's Republic of China, Turkey, and the United Arab Emirates to facilitate the transfer of technology and military equipment of foreign manufacturers. (**ways**).

The sanctions imposed by the U.S. Department of the Treasury have included companies from the three countries because confirmed imports of technology were identified, as follows:

No.	Country	Imported products
1.	Turkey	- electronic integrated circuits, ceramic capacitors, lithium-ion batteries, electric batteries, electronic integrated circuits and machines for data transmission and regeneration
2.	People's Republic of China	- telecommunications equipment, laser and radar components for anti-aircraft missiles
3.	United Arab Emirates	- equipment for the aviation industry, aviation equipment and technology - financial intermediation and investment services through ARX Financial Engineering Limited, a company that has identified ways in which Russian rubles could be converted into US dollars

The actions of those involved in aiding Russia through these supplies were sanctioned by the Office of Foreign Assets Control (OFAC) through the issuance of executive orders specifying the blocking of property regarding specified harmful foreign activities of the Government of the Russian Federation. (OFAC, 2022)

The economic sanctions from the European Union have prompted the Russian Federation to change its strategy for exporting petroleum products, shifting towards China, India, and Turkey.

We can conclude that the significant advantage of Russia's aggression against Ukraine lies in the location of the events. The war fought on Ukrainian territory has stimulated the aggressor's economy through increased demand for goods, services, arms and ammunition production, and labour force. In parallel, Russia has redirected its exports to China and India to mitigate the impact of economic sanctions imposed by the European Union and the United States. Alex Isakov, a former economist for Russia and current specialist at Bloomberg Economy, stated that the Russian Federation is capable of sustaining the war for another two years at the cost of an oil export price of $50 per barrel. (Huileng, 2024)

5. The financial instrument

It emerged during the war on terrorism as the United States sought to disrupt and dismantle global terrorist financial networks. (Harland, 2015)

The most prominent example of financial sanction applied to the Russian Federation was in 2023 when Russian banks were no longer able to use SWIFT (Society for Worldwide Interbank Financial Telecommunication) to transmit financial information when transferring funds to Russia. Instead, they were required to use only Russian services and internal financial infrastructure for these operations, according to the requirements of the Central Bank of Russia. (Interfax Group, 2023) This measure has a significant impact on the war strategy, as the SWIFT system brings together over 11,000 financial institutions from more than 200 countries.

The alternative to these restrictions for the Russian Federation has been both the promotion of an alternative payment system based on rubles called the System for Transfer of Financial Messages (SPFS), as well as the Cross-Border Interbank Payment System (CIPS) in China, which processes payments in Chinese yuan. (Huileng, 2022) (**means**)

We conclude this analysis with a grim forecast regarding global inflation and the recession determined by the connection between oil prices, international industries, and product prices. Russia supplies 40% of the EU's gas, and its price has increased by 50% since the beginning of the aggression in 2022. The rise in gas prices will lead to a decrease in industrial activity (temporary business stagnation) and an increase in food prices. The inflation thus determined will be felt globally through reduced purchasing power.

6. The Intelligence instrument

In the period leading up to the extensive invasion of Ukraine, the United States and the United Kingdom identified information about the invasion, publications, and forces from external sources, such as Bellingcat. We can analyse the importance of information, as seen in the example from February 24, 2022, when Professor Jeffrey Lewis from the Middlebury Institute examined traffic reports on Google Maps to identify a blockade on the Russian side of the border at 15:15 on February 24, just three hours before the invasion began. (Musumeci, 2022)

Open-Source Intelligence (OSINT) has had a considerable impact on military intelligence, information warfare, media reporting, and documenting war crimes. Defined as "the practice of collecting and analysing information gathered from open sources to produce actionable intelligence," (Gale, 2023) OSINT offers a significant advantage in that the types of available sources are incredibly diverse. Data can be collected, processed, and analysed from commercial satellite imagery, public posts on social networks, unencrypted radio messages, and other publicly available sources.

The use of OSINT in the Ukraine war quickly becomes an important case study for future practitioners in the field of intelligence and decision-makers. One of the reasons the war in Ukraine has turned into a trench warfare scenario after two years of conflict is the underestimation of the adversary and the lack of analysis regarding the will of the people to defend themselves. On the other hand, Russia's overestimation of its own capabilities turns it into an actor that learns what a large-scale ground operation entails. The political objective has expanded after 2 years to include regime change in Kiev. (**ends**)

In conclusion, Russian military intelligence learns from past failures, focusing its activities on NATO member countries. We recall instances such as the poisoning of Alexei Navalny, the overestimation of Russian capabilities prior to the invasion of Ukraine, and the expulsion of intelligence agents from embassies. Certainly, in 2024, this apparatus will infiltrate Europe more effectively, collaborating with Muslim communities in the region. Furthermore, the cyber threat to critical global infrastructure will bring Chinese, Russian, and Indian networks to the forefront.

7. The law instrument

The aspect of enforcing international legal provisions requires agencies to work closely through the diplomatic instrument of power, using data from the intelligence instrument of power, to track offences and conduct activities at a tactical level, including through the military instrument.

Several international organizations, including the International Criminal Court (ICC or "the Court"), the United Nations, the Organization for Security and Cooperation in Europe (OSCE), the European Union (EU), and human rights organizations, have identified cases of potential Russian war crimes in Ukraine.

It is assumed that Russian forces have committed crimes, arbitrary detentions, forced disappearances, interrogations, and reprisals against the civilian population of Ukraine. Some violence against civilians appears to have been carried out by individual soldiers and units, while in other cases, Russian forces have conducted systematic and coordinated operations to suppress and eliminate opposition to Russian domination in the areas they occupy. (Freking, 2023). These operations seem to be overseen by senior Russian political and military authorities.

In cases documented by the Office of the United Nations High Commissioner for Human Rights (OHCHR), over 91% of civilian detainees held by the Russian Federation described being subjected to torture and ill-treatment, including sexual violence. In the documented cases, such treatment appeared to be carried out to force victims to confess to assisting Ukrainian armed forces, to compel them to cooperate with occupying authorities or to intimidate those considered to hold pro-Ukrainian views. In many locations, the detention conditions have been so horrifying that they have been likened to torture according to international law. (OHCHR, 2023). The list of atrocities committed by the Russian Federation throughout this war includes sexual violence, abduction of children, mistreatment of prisoners of war, and artillery strikes on civilian targets.

We can conclude that the Russian Federation has enacted domestic laws revealing a desire to suppress dissent among the population. These laws define sabotage, terrorism, or extremism, with punishments that can reach up to 20 years of imprisonment.

Conclusions

It is true that wars end, but not all end in the same way. Some end through negotiation, while others end in capitulation. Following a brief analysis of the international measures applied to the Russian Federation in the past two years, we can make a prediction regarding aggression for the year 2024, through the lens of diplomatic, informational, military, economic, financial, informational, and legal instruments.

The objective of expelling Russian diplomats or active intelligence agents has been to isolate the Russian Federation, including limiting access to international bodies from the Council of Europe to the International Labour Organization or, most recently, the UN Human Rights Council. However, the BRICS group will include in 2024 Egypt, Ethiopia, Iran, Saudi Arabia, and the United Arab Emirates. In this situation, both the President of the Russian Federation and that of Ukraine are seeking an "exit strategy" that does not compromise their honour and involves making as few concessions as possible. The diplomacy through which future peace will be negotiated will likely involve considerations such as ceding Crimea to Russia and exploring options regarding the fate of Donbas.

From an informational perspective, the year 2024 will be a decisive point on the political stage. The Russian Federation will exert all efforts to destabilize the world order through hybrid attacks on presidential elections in both the United States of America and Russia.

From a military standpoint, Russia will take advantage of the current war of attrition to regenerate its forces, initiate recruitment drives, and transition to offensives in the summer-fall campaigns of 2024, following the presidential elections. The projected military expenditures for this year will surpass those allocated to social needs, although it is superior to Ukraine's in terms of equipment, weapons, ammunition stocks, aircraft, and electronic warfare capabilities for a considerable period.

Russia's economy seems to gain billions from exports of oil and diamonds, but it faces inflationary problems. Inflation is fueled by the devaluation of the ruble due to economic sanctions, leading to price hikes. The promise of allocating 6% to the military domain (Luzin, 2023) confirms that the war is not nearing its end in 2024.

The conclusion of this article is that the influence of artificial intelligence (AI) developed by the Russian Federation in 2024 will enhance the efficiency of military technology, provide real-time prediction of operations and facilitate international cyber operations, in the context of global presidential elections. However, through various means, Russia will achieve its desired end state of territorial expansion, at the risk of disrupting the world order and the cost of human lives, but it will remain an enigma shrouded in mystery, according to the definition received in 1939.

BIBLIOGRAPHY:

1. Alexander E. Gale ”*The Role of Open-Source Intelligence in the War in Ukraine*”, 2023, available at https://moderndiplomacy.eu/2023/05/17/the-role-of-open-source-intelligence-in-the-war-in-ukraine/, accessed on 04 February 2024.
2. Bhavya Sukheja ”*Ukrainian Forces Find Russian Sea Mines Near Odessa Coast After Storms*”, 2022, available at https://www.ndtv.com/world-news/russia-ukraine-war-ukrainian-forces-find-russian-sea-mines-near-odessa-coast-after-storms-2982998, accessed on 30 January 2024
3. Christian Perez, ”*Information Warfare in Russia's War in Ukraine*”, 2022, available at https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/, accessed on 25 January 2024
4. Derek S. Reveron ”*When diplomacy goes to war*”, 2023, available at https://www.fpri.org/article/2023/04/when-diplomacy-goes-to-war/, accessed on 25 January 2024.
5. Dobrin Dobrev, ”*Security Challenges in the Black Sea: Military Exercise or a Navy Blockade? Analysis of the Russian Navy Activities in Bulgaria's Exclusive Economic Zone in the Black Sea*”, 2023, available at https://opiniojuris.org/2023/11/10/security-challenges-in-the-black-sea-military-exercise-or-a-navy-blockade-analysis-of-the-russian-navy-activities-in-bulgarias-exclusive-economic-zone-in-the-black-sea/, accessed on 07 February 2024.
6. Edward Malnick ”*Inside the secret government unit returning fire on Vladimir Putin's 'weaponised lies*”, 2022, available at https://www.telegraph.co.uk/news/2022/03/19/ inside-secret-government-unit-returning-fire-vladimir-putins/, accessed on 25 January 2024
7. European Commission guidelines on the oil market ”*Price Cap Coalition statements and guidance*”, 2023, available at https://finance.ec.europa.eu/publications/price-cap-coalition-statements-and-guidance_en, accessed on 03 February 2024
8. Execution orders issued by the Office of Foreign Assets Control, ” *Russian Harmful Foreign Activities Sanctions*”,2022, available at https://ofac.treasury.gov/faqs/ topic/6626, accessed on 03 February 2024.
9. Florin Nistor, Lucian-Valeriu Scipanov, ” *Influența caracteristicilor Mării Negre asupra Operațiilor Întrunite*”, Strategic Impact, 2021, p. 30
10. Foreign Commonwealth & Development Office, ”*UK and allies sanctions Russian cyber hacker”,* 2024, available at UK and allies sanctions Russian cyber hacker - GOV.UK (www.gov.uk), accessed on 05 February 2024.
11. General Assembly resolution demands end to Russian offensive in Ukraine, 2022, available at https://news.un.org/en/story/2022/03/1113152, accessed on 25 January 2024.
12. Heather Mongilio ”*Turkey Closes Bosphorus, Dardanelles Straits to Warships*”, 2022, available at https://news.usni.org/2022/02/28/turkey-closes-bosphorus-dardanelles-straits-to-warships, accessed on 30 January 2024
13. Huileng Tan, ”*How Russia has avoided bankrupting itself after 2 years of waging war in Ukraine*”, 2024, available at https://www.businessinsider.com/russia-economy-how-moscow-pays-war-economy-afloat-sanctions-ukraine-2024-2, accessed on 20 February 2024.

14. Huileng Tan, ” *China and Russia are working on homegrown alternatives to the SWIFT payment system. Here's what they would mean for the US dollar.”,* 2022, available at https://www.businessinsider.com/china-russia-alternative-swift-payment-cips-spfs-yuan-ruble-dollar-2022-4, accessed on 07 February 2024.

15. Interfax Group ” *Russian banks banned from using SWIFT for transfers within Russia as of October 1*”, 2023, available at https://interfax.com/newsroom/top-stories/95043/, accessed on 07 February 2024.
16. Ionuț Cioranu, ”*Gândirea critică în leadershipul militar*”, Universitatea Națională de Apărare ”Carol I”, Colocviu Strategic, 2021
17. John Crace ”*Russia bans Facebook and Instagram under ‘extremism’ law”*, 2023, available at https://www.theguardian.com/world/2022/mar/21/russia-bans-facebook-and-instagram-under-extremism-law#:~:text=A%20Russian%20court%20has%20 banned,on%20western%20social%20media%20giants., accessed on 25 January 2024
18. Joint Publication (JP) 1, Doctrine for the Armed Forces of the United States, 2018, p 26 , available at https://irp.fas.org/doddir/dod/jp1.pdf, accessed on 30 January 2024
19. Kevin Freking ”*Ukraine’s top prosecutor speaks of ‘evil’ Russian atrocities*”, 2023, available at https://apnews.com/article/congress-ukraine-russia-war-crimes-torture-1015b6b6393489d088b0980225ff4509#:~:text=%E2%80%9CSuch%20evil%20cannot% 20let%20be,the%20land%2C%E2%80%9D%20Kostin%20said., accessed on 07 February 2024.
20. LCDR Harland A. Hendricks, USN, ”*Modern Financial Warfare: Drawing on Lessons from the Globalized Economy Pre-World-War I”*, 2015, available at https://apps.dtic.mil/sti/trecms/pdf/AD1175878.pdf, accessed on 03 February 2024.
21. Marcus Lu, *”Visualizing the BRICS Expansion in 4 Charts*”, 2023, available at https://www.visualcapitalist.com/visualizing-the-brics-expansion-in-4-charts/ , accessed on 20 January 2024.
22. Mykhaylo Zabrodskyi, Jack Watling, Oleksandr V Danylyuk and Nick Reynolds ”*Preliminary Lessons in Conventional Warfighting from Russia’s Invasion of Ukraine: February–July 2022*”, available at https://static.rusi.org/359-SR-Ukraine-Preliminary-Lessons-Feb-July-2022-web-final.pdf accessed on 30 January 2024
23. Natalie Musumeci ” *A California professor says he spotted Russia's invasion of Ukraine on Google Maps hours before Putin announced the attack*”, 2022, available at https://www.businessinsider.com/professor-says-he-saw-russia-ukraine-invasion-on-google-maps-2022-2, accessed on 07 February 2024.
24. Pavel Luzin, ” *Russia’s 2024 Budget Shows It’s Planning for a Long War in Ukra*ine”, 2023, available to https://carnegieendowment.org/politika/90753, accessed on 09 February 2024.
25. Ralph S. Clem ”*What exactly is Putin’s new ‘New Russia’?*”, 2014, available at https://www.washingtonpost.com/news/monkey-cage/wp/2014/09/04/what-exactly-is-putins-new-new-russia/, accessed 22 January 2024.
26. Richard Martin, ”*Sanctions against Russia – a timeline”*, 2023, available at https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/sanctions-against-russia-8211-a-timeline-69602559, accessed on 31 January 2024
27. Russian News Agency ” *Nearly 600 Russian diplomats expelled from Western countries since February 2022*”, 2023, available at https://tass.com/politics/1567203, accessed on 05 February 2024.
28. Tayfun Ozberk ”*Russia’s Amphibious Operation Dilemma*”, 2022, available at https://www.navalnews.com/naval-news/2022/03/russias-amphibious-operation-dilemma/, accessed on 30 January 2024
29. The Rt Hon Boris Johnson, ” *PM statement on the situation in Ukraine: 22 February 2022*”, 2022, available at https://www.gov.uk/government/speeches/pm-statement-on-the-situation-in-ukraine-22-february-2022, accessed on 22 January 2024.
30. The Associated Press ”*Putin: Russians, Ukrainians are ‘one people*”, 2019, available at

https://apnews.com/article/3fe3ff2299994fae97825381765b831c, accessed 22 January 2024.

31. U.N. Office of the High Commissioner for Human Right (OHCHR), ”*Detention of Civilians in the Context of the Armed Attack by the Russian Federation Against Ukraine, 24 February 2022–23 May 2023*”, 2023, available to https://reliefweb.int/report/ukraine/detention-civilians-context-armed-attack-russian-federation-against-ukraine-24-february-2022-23-may-2023#:~:text=OHCHR%20documented%20864%20individual%20cases, also%20amounted%20to%20enforced%20disappearances, accessed on 07 February 2024.
32. U.S. Air Force, ”*The Joint Team*”, 2022, available at https://www.doctrine.af.mil/Portals/61/documents/Airman_Development/PurpleBook.pdf, accessed on 15 February 2024.
33. ”*Winston Churchill's first wartime broadcast”,* available at https://www.bbc.com/historyofthebbc/anniversaries/october/winston-churchills-first-wartime-broadcast, accessed 17 January 2024.

SECTION 2

TECHNOLOGIES – MILITARY APPLICATIONS, CYBERDEFENCE, MODELLING AND SIMULATION

1053477-3045-1396-24-12

RESPONSE CELL – A CORNERSTONE IN PLANNING AND CONDUCTING A COMPUTER-ASSISTED EXERCISE

Diana-Ioana ZINCA-EMCH, PhD.
Maj. PhD. in Military Science domain, Staff Officer at National Defence University,
Bucharest, Romania
E-mail: zinca_diana@yahoo.com

Ghiță BÂRSAN, PhD.
BGEN, Prof. Eng., Commandant (Rector), „Nicolae Balcescu" Land Forces Academy,
Sibiu, Romania
E-mail: ghbarsan@gmail.com

Abstract*: The war in Ukraine directly impacted NATO's security architecture and emphasized the importance of maintaining training at a high level not only for the Alliance's high-readiness forces, but also for all NATO force elements. By establishing multinational battlegroups in the eastern part of NATO's territory, it became necessary for local and NATO troops to train together to be able to fight together, if needed. Over the years, NATO forces located in Romania have constantly trained with both Romanian and Bulgarian units as part of their annual exercises, where local troops were regularly assigned as response cells for NATO forces. Recognizing the vital role played by response cells and overcoming obstacles encountered during planning and conducting these exercises, we have developed this research paper to guide response cell units toward better supporting NATO exercises.*

Keywords: *Response Cell (RC), Exercise Control (EXCON), Computer Assisted Exercise (CAX), Functional Area Services (FAS), Main Event List/ Main Incident List (MEL/MIL).*

Introduction/Preliminary considerations

Planning a NATO exercise is a manifold process that requires up to a 24-month period, based on the level of ambition and the complexity of the exercise. In the last 5 years, we noticed NATO's increased interest in merging live exercises into Major Joint Operations Computer Assisted Exercises (CAXs), offering a wider variety of training for all levels of units. It is clear that multi-level training is a priority for NATO exercises, and it can be seen during exercises such as Loyal Leda 2022, where both the NATO Multinational Division South-East and NATO Multinational Corps South-East were secondary training audiences or the four-level exercise STEADFAST JUPITER 2023 when NATO Multinational Corps South-East reached its final operational capability. These types of exercises are training both NATO and national units in conducting multi-domain operations and testing the Alliance's defence posture and warfighting readiness. Those exercises are also the perfect example of major training events in which national units from NATO countries play an important role in supporting NATO exercises. For instance, during LOYAL LEDA 2022 both Romanian and Bulgarian brigades were Response Cells (RC) for NATO Multinational Division South-East, while a Romanian Division level unit played the RC role for NATO Multinational Corps South-East in both exercises. We are confident that having a basic understanding of the RCs' roles and responsibilities during planning and conducting a NATO exercise will help the national units to better support the exercise. In aiming to improve the exercises' support, we developed this research paper that starts with the definition of the RC and explains the architecture of the exercise with the RC's role and place in it. Furthermore, this paper presents the involvement of RC units during the planning process of an exercise and the deliverables expected from them. Finally, the last chapter highlights the important role of an RC during the conduct phase of the exercise. The last chapter can also be seen as training for upcoming RCs. It explains in detail the RC's structure, the exercise framework, the tools used by the RC during the exercise, the information flow within the RC, and also the link between the Main Incident List/ Main Event List (MEL/MIL), the simulation (SIM) systems used during the exercise and the RC operators. Bottom line: this paper aims to provide knowledge for the RC personnel from the perspectives of both NATO training directives and best practices used in NATO exercises. This will give the RC's personnel a solid understanding of their role in the exercise, will improve their performance, and will better help in supporting the exercise.

II. The RC's role and place within the exercise structure

When we speak about an exercise, our minds immediately go to the people who get trained, the Training Audience (TA). They are the primary focus, the reason why the exercise has been built in the first place. However, in this research paper, we are going to speak about the importance of the body that controls the exercise (Exercise Control- EXCON) and make sure that during the exercise the TA can reach their Training Objectives (TOs). To better understand the scale of an EXCON during the conducting phase of an exercise, please take a look at Fig no. 1, which provides a glimpse into the exercise's environment.

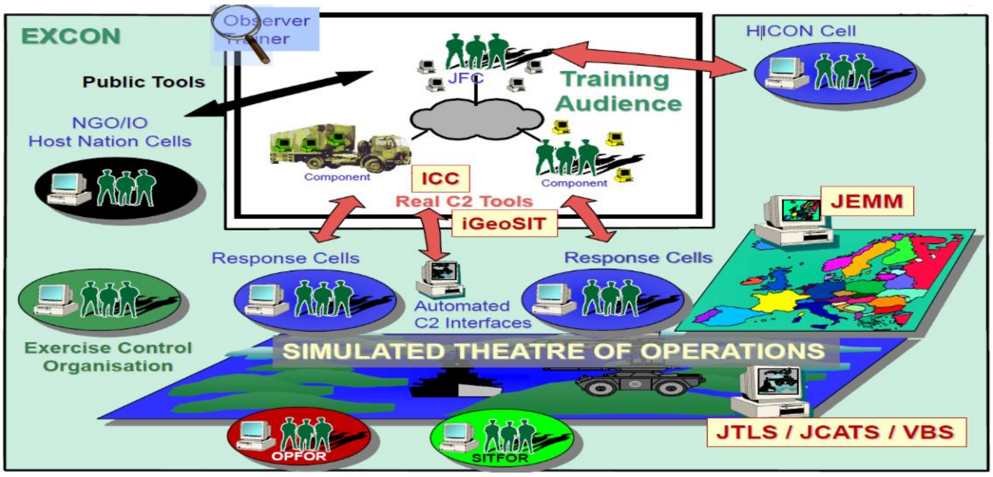


Figure no. 1. The exercise's framework [1]

The TA is depicted as the core of the exercise; they are immersed in a virtual battlespace built by the simulated systems used for training and the arrows between the blocks highlight the fact that to meet their TOs, the TA is supported by all of the EXCON's entities.

In the NATO BI-STRATEGIC COMMAND DIRECTIVE 075-003 (BI-SCD 75-3), "EXCON is the term used to describe all of the participants during the conduct of Collective Training and Exercise (CT&E) activities who are not in the TA and thus are under the control of the Exercise Director (EXDIR)"[2]. A generic EXCON structure is presented in Fig. no.2 and it usually includes: the support staff for the EXDIR; the exercise's support elements (Communication and Information Systems (CIS), Real Life Support, public information and visitors bureau); the training teams (TT) and mentors; the exercise Centre (EXCEN) comprising of situation control (SITCON) elements (Opposing Forces (OPFOR), scenario, MEL/MIL management and CAX Support teams); the response cells (higher (HICON), neighboring (SIDECON) and lower situational forces (LOCON) and non-NATO entities like grey cell and simulated press (SIMPRESS)).

The EXCON is directed by the EXDIR on behalf of the Officer Conducting the Exercise (OCE). [2]

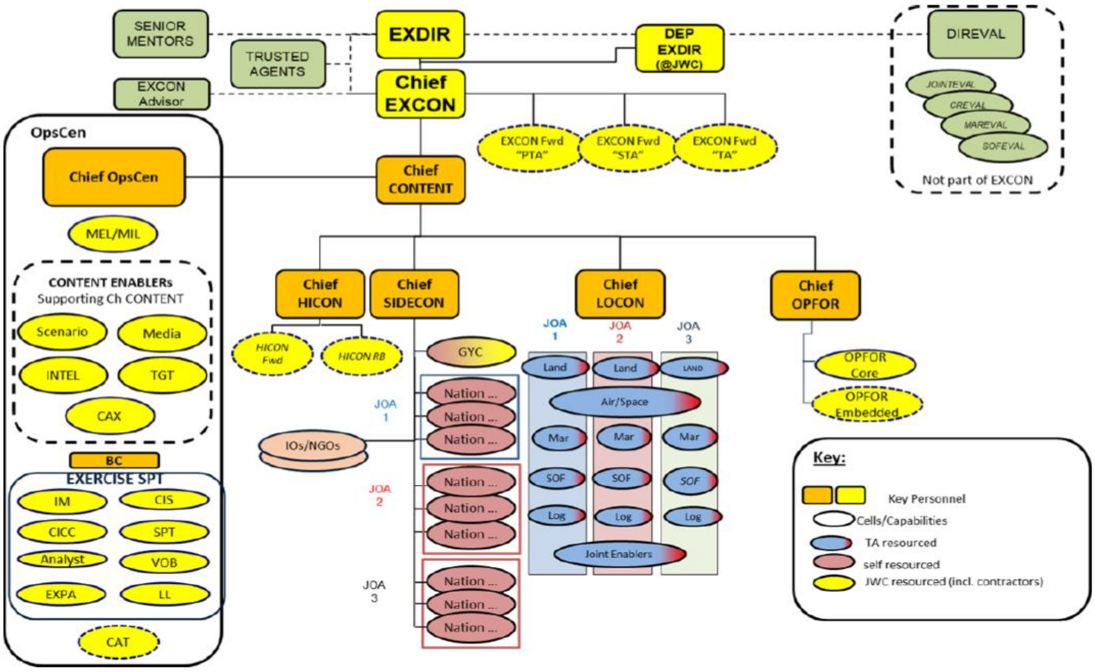


Figure no. 2. Generic EXCON organization for training [2]

Now that the role and responsibilities of the EXCON during the conduct phase of an exercise have been identified, our research goes deeper and starts focusing only on the RCs and their support during both the planning and conducting of an exercise. The NATO BI-SCD 75-3 defines four possible levels of participation in an exercise: Primary Training Audience (PTA), Secondary Training Audience (STA), Robust Response Cells (R-RCs) and RC. The RCs are defined as all subordinated HQs that receive guidance from TA, they have a symbolic participation in the exercise and provide minimal interaction with the TA during the conduct phase of the exercise, and basically, they respond to the TA requirements only in the main capability areas. The R-RCs are bigger RCs that can train their internal procedures, run their battle rhythm and respond to TA solicitations as realistically as possible in all functional areas. It is important to understand from the beginning that when we speak about RCs in this paper, we refer to both RCs and R-RCs.

The RCs are all the units that during the conducting of the exercise receive guidance or orders from the TA (their subordinated HQs- LOCON) or that interact with the TA (higher HQ-HICON, SIDECON, grey cells or SIMPRESS). They represent the troops on the ground, the military equipment, vessels, aircraft, and all the entities that are simulated on the battlefield. The RCs are interacting with the TA through reports and returns sent by the Command and Control (C2) tools that the TA is using (fig.no.1). Nevertheless, it is very important to emphasize the fact that the RCs's goal is to support EXCON and push the TA to reach their TOs. The quality of the exercise depends on the RCs' support, knowledge and understanding of the exercise framework, situation, and the TA's TOs. During the conduct of an exercise, the RCs' personnel must support both EXCON and TA Battle Rithm (BR) events. Being part of the RC feels like working for two bosses at the same time. As LOCON, you need to follow the operational orders received from your higher echelon (the TA) and at the same time, from the exercise perspective the RC remains under the Officer Directing the Exercise's (ODE) command to reach the exercise TOs. As depicted in figure no.2, the RCs are subordinated to the ODE, which is also the EXDIR and operates and organizes EXCON. This means that to properly support the exercise, all the RC personnel need to understand their role within

EXCON, the TA's TOs, the MEL/MIL script and they also need to be experts in their field because they replicate the functions of the TA subordinate forces. Therefore, the RC workforce structure and composition are carefully considered. The discussions regarding the RC composition start at the exercise Initial Planning Conference (IPC) and are finalized after the analysis of the MEL/MIL script. The RC is led by the RC Chief, who is assisted by the Battle Captain who is also acting as his Deputy. All the other functions from the RC are covered by qualified personnel. The RC core functions are identified based on the TA TOs and the MEL/MIL scripting. For example, a Land RC for the Division level usually has 12 PAX (2-3 PAX Intel, 5 PAX Operations Plans, 3 PAX Logistics), plus 4 PAX per Brigade. Part of the RC will also be the CAX operators who might be provided by the training center and if possible, a MEL/MIL coordinator.

Since the RC personnel need to understand the MEL/MIL scripting in order to be able to support the exercise, it is clear that their input and support start from the exercise's planning phase. In the next chapter, we will speak about the RCs' involvement in the exercise planning process and the deliverables they are expected to develop.

III. The RC's involvement in the exercise process

The exercise process is very complex; the planning process takes up to two years and is comprised of 4 stages: Stage 0: Initiation, Stage 1: Specification, Stage 3: Planning and Stage 3: Conduct. Each of these stages has a clear timeline and deliverables that need to be developed to build the exercise.

Stage 0 is preparatory in nature, it sets the stage for developing the exercise by identifying key responsibilities and setting the level of ambition for the exercise, as well as the resources that can be allocated for it. This stage is led by the Officer Scheduling the Exercise (OSE) and the primary deliverable of Stage 0 is the Exercise's Initiation (EXINT) slides-package which contains the Exercise Aim (EA) and the draft Exercise Objectives (EOs).

Stage 1 starts developing more details and expounds the exercise ambitions, resources, roles, and responsibilities outlined in the EXINT. The deliverable of this stage is the Exercise Specifications (EXSPEC), a document that binds the key stakeholders by connecting the exercise participation, including supporting HQs (RCs) and organizations around EAs and EOs. The EXSPEC is basically the foundation for the exercise planning, it can be seen as an order from the OSE to the OCE to plan, conduct and analyze the exercise. It is usually released 12-18 months prior to Stage 3 (Conduct) to establish the resources' availability and participation of TA, supporting HQs (RCs) and organizations, funding, CIS, Host Nation and Partners. If an HQ decides to play the RC role within an exercise, their engagement appears in the EXSPEC. Due to the fact that the EXSPEC is a justifying document for budget allocation and delineation of roles and responsibilities, it means that the HQ that committed to being a RC in an exercise understands the following: they will have to be part of different conferences or workshops during the planning stage, they will contribute to developing the Order of Battle (ORBAT), during the conducting stage of the exercise they can either use ODE workspace or deploy to a location that was previously agreed upon, and they are eligible for partial or full transport reimbursement but the individual nations are paying the Per Diem which includes the meals and accommodation. Bottom line: the participation of an HQ or organization as an RC in an exercise is usually established before the EXSPEC is delivered.

Stage 2 is led by the OCE and covers all the planning activities that will support the delivery of the CT&E activities scheduled for Stage 3. The Exercise Plan (EXPLAN) is the primary deliverable for the Planning stage. It explains in detail the exercise's preparation and execution based on the OSE guidance. Other major deliverables of this stage are the TOs, the Scenario Modules, the OCE Guidance, the exercise participation/ CAX support preparation and the MEL/MIL. During this stage, the RCs have the obligation to contribute to MEL/MIL development and the CAX Database (DB) Validation meeting. The DB validation is generally conducted 6 weeks before the beginning of the exercise (STARTEX) and it always takes place before the MEL/MIL Scripting Conference. The major data providers participate at the workshop for 2-3 days, being supported by experts from the training center. The validation session's purpose is to run the simulation system with the exercise database. The tests are conducted in order to ensure that all the inputs from the database (units, equipment, targets and terrain) behave and interact in a realistic manner. By attending this meeting, the RC representative makes sure that all his units' assets (from ORBAT) are replicated within the CAX DB, are simulated accurately and act in a realistic way. It is important to highlight the fact that in a CAX the simulation systems feed the C2 systems used by the TA. This means that the Common Operational Picture (COP) is built by the simulation system, based on the assets and the capabilities that each unit possesses. All the information regarding the units' capabilities and assets is listed in the ORBAT. The importance of DB Validation meeting is obvious now: if the ORBAT data provider doesn't make sure that all his units' assets are replicated correctly in the simulation system, then during Stage 3 of the exercise the TA will not have a realistic COP and the reports and returns received from the simulated systems will not be accurate. Therefore, the RC personnel will not be able to respond to the TA requirements or properly support the exercise. Another meeting takes place in the Planning Stage of the exercise and the RC personnel are required to participate in the MEL/MIL Scripting workshop.

At least 4 weeks prior to Stage 3, the RCs are usually invited to participate in the MEL/MIL scripting workshop to develop injects for the TA in the Joint Exercise Management Module (JEMM). Within this workshop, the personnel will create "problems" for the TA to push them to achieve their TOs. The MEL/MIL is the main tool that pushes the TAs to reach their TOs. Without the MEL MIL part, the exercise is no more than a video game. "The MEL/MIL is stored in the JEMM system and during the conduct phase of the exercise, it is presented to the TA through injects/ reports which will trigger decisions and will generate specific effects in order to provide the most accurate training opportunities." [4] The MEL/MIL is the best way to track the TAs' performance during Stage 3 and in the end even helps with the assessment of how many of the TOs were played and met by the TA. The JEMM provides these types of reports which are used for the exercise feedback. It is critical that the personnel that attend the Scripting Workshop also be part of the RC personnel during Stage 3 to have a clear understanding of the MEL/MIL DB and be able to support it and dynamically script other injects if needed.

Stage 3 is divided into a sequence of six training blocks which, within the available resources and the EXCON's supervision, will help the TA to meet their training requirements listed in EXSPEC. The first *training blocks, A (Academics) and B (Battle Staff Training)* are the TA's responsibility, but if needed the EXCON's personnel (experts from the training center) can provide support or advice. Usually, the RCs do not take part in these two training blocks. *During the C-block (Crisis Response Planning – CRP)* though, the RCs involvement will be required. In block C, the TA trains their operational planning process and they will develop operational documents (OPLAN, OPORDER, etc.). Part of the RC personnel might be invited to participate in some meetings during the TA's Operational Planning Process (OPP) to make sure that the subordinate units understand the TA Commander's vision and plan. After the OPLAN is developed, based on the agreed involvement of the RC in the exercise (R-RC or just a RC), they are required to produce some robust operational plans/ orders. If the RC personnel are not familiar with the real C2 systems that the TA is using, then somewhere between training blocks A and C, the TA can offer training on systems for their subordinate units. If that training will not be enough, before training block E, during EXCON training, the RC personnel can request another session of training on specific FASs. As is depicted in Fig. no.1, the TA uses during the execution of the exercise the C2 systems that they normally use every day at work (LOGFAS for logistics, Intel

FS for Intel, JTS for targeting, etc.). The reports and returns, updates, and each interaction that RC personnel have with the TA during the exercise take place through those FASs. Therefore, is crucial for the RC personnel to have at least user-level training on the FASs that are used during the exercise.

Training block D (Deployment Exercise- DEPLOYEX) refers to the deployment, execution of Force Activation and the Reception, Staging and Onward Movement (RSOM) process. Based on the nature of the exercise, the EOs and TOs, this training block can be the exercise itself or it will not be played at all. If it is played at a large scale, the roles and responsibilities of EXCON personnel are the same as for training block E.

During *training block E (Employment Exercise- EMPLOYEX)* a selected timeframe or timeframes of the OPLANs developed by the TA during training block C are executed. It represents the execution and conduct of operations. "The TA executes the planning and conduct of operations in order to develop operational and procedural skills, to enhance HQ/force readiness, to develop HQ/forces interoperability, and to deliver Strategic messaging (when applicable)." [2] This training block is under EXCON control to make sure that the TA is reaching their training requirement. This is the part where Modeling and Simulation (M&S) technology is "used to immerse the TA in a realistic environment and to help the exercise planning group and the exercise control staff in controlling the exercise process so that it achieves the objectives effectively" [6]. The RC's involvement in training block E will be detailed in the next chapter.

The last training block is F (Follow-on training). This training block is not for reaching TOs or completing evaluation criteria. It represents the opportunity for commanders to address lessons identified or any other concerns acknowledged during the planning or execution of the exercise. Based on the requirements and the timelines established in EXSPEC, the OCE and ODE can provide the TA the opportunity for additional training on the above-specified issues, however, that training will be limited to a tabletop exercise or wargame. Taking into consideration the small scale of this training block, the RC personnel will most likely not be involved.

This chapter provided a broad understanding of RC's involvement in all stages of the exercise process. In the last chapter of this research paper, we will explain in detail the RC's involvement during training block E, the information flow within the RC and how it supports the TA during the execution of the exercise.

IV. RCs' support during Training Block E

Throughout this research, we have constantly referenced and explained two key figures. Figure no.1 represents the exercise's Block E architecture. Upon taking a closer look, you will identify not only the main actors in an exercise (TA and EXCON), but also the systems used both for supporting the exercise (EXCON tools) and the C2 systems used by the TA. In the middle is the TA, who gets trained in conducting operations and they are using C2 systems IOT coordinate with the higher and lower echelons (which are depicted as RCs). Everything that is in the blue box is part of EXCON and their job is to keep the exercise up and running and support the TA to achieve their training objectives. It is very important to understand that TA has access to neither the JEMM (MEL/MIL DB), nor to the simulation systems (JCATS/JTLS). Those are EXCON tools only. The tools that TA use during block E training are: NATO Secret (NS) / Mission Secret (MS) workstations; Telephones/Fax; C2 Systems = FASs like LOGFAS, NCOP/LC2IS, Intel FS, JTS, etc.; Maps; Battlespace information (OPLANs, OPORDERs).

EXCON uses all the same tools that the TA does, plus the simulation system workstations and scenario information and MEL/MIL DB in the JEMM. In conclusion, "TA works with C2 systems while response cells use JCATS/ JTLS in order to simulate the battlefield, JEMM to inject the events and the FASs to maintain the information workflow within the organization" [3]. We stated before and it can be seen in Figure no.1 that the simulation systems automatically build the COP for the TA in NCOP/ LC2IS or whatever other FAS the TA uses. During the planning stage of the exercise, the CAX team makes sure that the simulation DB is synchronized with the C2 system DBs. The simulation systems provide the ground truth in an exercise, and they deliver only a perceived view of the situation based on available intelligence efforts and assets that the units have. This means that the TA will see on their COP only the things that they are allowed to see, based on the collection assets that they have listed in the ORBAT. Moreover, the simulation systems provide feedback reports such as personnel reports, enemy detection, battle damage assessment (BDA), etc. Those reports are sent as feedback to the TA by the RC personnel. Before explaining the information flow within an RC and how the COP is built by the simulation systems, we need to explain the link between the MEL/MIL DB and the simulation systems. The MEL/MIL DB is built during the planning stage of an exercise to achieve the training effect required by the TA; the TOs that they want to reach. The MEL/MIL will provide the TA stories to support each area/ domain that the TA wants to train. For instance, some things cannot be replicated in the simulation, like civilians or the media's impact on the operations. To train TA's reaction to this type of problem, stories are created during MEL/MIL workshops to make sure that during training block E the TA has plenty of opportunities to achieve the required training. For the things that can be replicated in the simulation systems, the SIM and the MEL/MIL DBs must be coordinated because the SIM feeds the C2 systems (what TA can see). For example, if the RC plays an inject that involves action from the SIM (like a convoy destroyed by the ENY aviation), even if it is scripted in advance or manually scripted, it has to be coordinated with the OPFOR and OPFOR CAX team (to have an airplane to fly over the convoy) and after making sure that all those details are ok (inject – action inject), then it can be injected (sent to the TA). All this coordination takes place in advance during Stage 2 at the MEL/MIL Workshops and during the conduct phase of the exercise, between EXCON members. Now that we explained the difference between the tools used by TA and EXCON, the importance of MEL/MIL and simulation DBs synchronization and the fact that the COP is built by the simulation systems, is time to put all this information together and explain the RC's role in supporting training block E. Figure no 3 explains the information flow within a RC during the execution of an exercise and is the perfect example for visualizing how the simulation feeds the C2 systems.

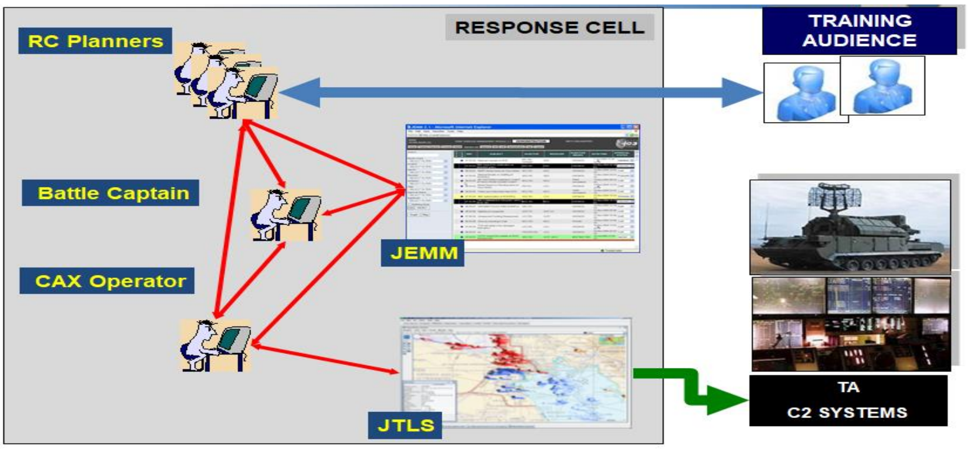


Figure no. 3. Information Flow within a RC [5]

The above figure represents the information flow between the RCs (HICON or LOCON) and the TA. The RC is led by the RC chief and the personnel comprises of the subject matter experts (SMEs)/ planners for each domain (logistics, intelligence, operations, etc), the Battle Captain and a CAX operator (who might be a contractor- with or without military background). As you can see, all the red arrows go to the Battle Captain. He is the center of the RC, the link between the planner, SIM and the MEL/MIL. All the inputs/ changes that are made in the simulation are checked first by the Battle Captain, then the CAX operator puts the orders into the SIM system. The reports that are pulled out of the SIM are sent by the CAX operator to the Battle Captain, and he is the one who disseminates them further to the SMEs. We are speaking about the reports and returns created daily by the SMEs in accordance with TA requests and battle rhythm. The reports are pulled out from the simulation, readjusted by the RC SMEs and sent to the TA through the C2 systems as daily reports (INTSUM, PERSREP, LOGREP, etc.). All the RC members have access to the JEMM, but with different rights (read-only, scripting, etc.). The person responsible for the MEL/MIL within the RC works in close coordination with the Battle Captain to make sure that all the injects are aligned with the operation. The information flow goes as follows: TA tasks (through an operational order) the subordinate unit (in this case the RC), the order gets to the Battle Captain, he disseminates it further and the planners start working on it, if movement in the SIM is involved, then the CAX operator will be tasked to execute orders in the SIM. The outcome will be visible to the TA since the SIM automatically feeds the C2 systems (based on their capabilities).

The SIM and the MEL/MIL are linked through the CAX operator (SIM operator and action injects on the JEMM). Now we explain the last part of Figure No. 3: the synchronization between the MEL/MIL and the SIM. Right before an inject is scheduled to be carried out (sent through email/ telephone/ radio or any other FAS to the TA), the action inject is operated in the SIM system by the CAX operator. Once movement can be seen in the SIM system, the RC SME reports the incident to the TA, then the TA will be able to track it on the C2 systems (which are fed by the SIM). This method prevents confusion. If the action is not synchronized with the injection developed by the RC, the TA will not be able to see the incident on their COP, therefore they will disregard the report received from the RC. That will eventually lead to losing the desired training effect. Therefore, within the RC, synchronization is everything. Otherwise, they will fail to support the exercise.

Now that we've fully explained the RCs' role in an exercise, I am confident that is crystal clear why the RCs are a cornerstone in planning and conducting an exercise. The last part of our research, highlighted within the conclusion, contains some of the RCs' issues we observed during national, multinational and NATO exercises and some guidelines to overcome them.

Conclusions

In over seven years of planning and conducting national, multinational and NATO CAXs, we have had the opportunity to observe some of the problems faced by the EXCON and their impact on the TA, as well as had the chance to apply some of the lessons learned and have further assessed the results. Therefore, this last part of our research paper will point out some of the lessons identified regarding the support provided by the RCs in an exercise, ways to overcome them and our conclusions.

The most common problem faced by EXCON during training block E comes from the RCs' will to help the TA (which in real life is also their higher echelon). No matter how much it is emphasized during the EXCON training briefing that the RCs are under EXDIR lead during training block E, they are still mistakenly treating the TA as their commanding unit, even disregarding the EXCON Chief's orders. We observed that in most cases, these problems occur from lack of knowledge, poor training or just different mindsets and background experience rather than from bad intentions. The first challenge faced by EXON is with the RCs that are going into the exercise with the mindset "train as you fight". They tend to forget that their specific role is to follow the script, the MEL/MIL DB and to push the TA to reach their TOs and to act as subordinate units only (following only TA guidance even if that is in contradiction with the EXCON's Chief's orders). Not to mention when the RC personnel want to be extremely helpful to the TA and let the TA know in advance some of the incidents scripted in MEL/MIL (the problems that they will have to solve). It is obvious that this type of behavior will eventually lead to losing some of the TOs. We observed both types of problems during an exercise; both were eventually solved without jeopardizing the exercise, but we firmly believe that these issues can be addressed in advance and will no longer affect the conducting part of a CAX. From our experience with NATO exercises, it takes up to 3 days for the RCs to get used to their roles and responsibilities and to start properly supporting the TA (under EXCON Chief's orders). Either way, if we speak about small issues (fully understanding the way that the SIM and the MEL/MIL support the exercise, how to dynamically script an inject or whom to coordinate it with), or even the big problems highlighted above, the average time for the RCs to get on track is 3 days. For a NATO exercise that is usually 10 days long, this represents almost a third of the training time that the TA doesn't receive the proper support. Not to mention that a national or multinational Division level exercise is 3 days long. In this case, the exercise is put in danger. To overcome those problems, we believe it is important for the RCs' members to be trained on their upcoming role well before training block E. The EXCON training at the beginning of the exercise will refresh the RCs' personnel's knowledge, but their understanding of roles and responsibilities should be clear before arrival. All the RCs' personnel should be trained at least 4 weeks in advance, either by the TA OPR or the personnel that attended the MEL/MIL scripting workshop. This will ensure that they will be able to play their part correctly in the EXCON and properly support the exercise. As simple a solution as it may seem, this is still a problem that we observe during exercises.

Another problem that we have faced during national and multinational exercises is regarding the SIM and FASs DBs synchronization. The RCs realized at STARTEX that either they do not possess all the assets in the SIM DB or that some of the assets from the SIM are different from the ones listed in their FASs (LOGFAS for instance). At that point, there is not much that can be done. The coordination within the RC must be very tight, and the stress will double as well as the work that they must put in. The problems they might face include their units not operating properly in the SIM, which would affect TA's COP, or the reports that are pulled out from the SIM are not accurate, and the RCs' SMEs need to find one by one the equivalent of the assets reported by the SIM in their FASs and then report it further to the TA. We remarked that those DB synchronization issues appear only during the exercises that do not hold the DB validation meeting during the planning phase of the exercise either because it is disregarded or because it is not part of their planning directive. Nevertheless, our experiences with NATO exercises have demonstrated that validating the DB and establishing firm deadlines for delivering inputs for the ORBAT, as well as naming conventions for SIM and FASs DBs, are the solutions to these problems. During training block E, many things can go wrong. Some of them can be prevented, such as what we have highlighted above, but each exercise has its own particularities, and there are always new lessons to be learned and things to be improved upon. This research paper is part of a series that started back in 2018 with the publication of "Constructive simulation programs and NATO Functional Area Services applied in Computer Assisted Exercises" and was developed to explain in a simple manner the way that the systems work in an exercise, the MEL/MIL process, or the RCs' role within a CAX. Throughout my career as an exercise planner, I have identified weaknesses in knowledge concerning the planning and conducting of exercises, so we decided to address them in our research papers, specifically to help the exercise planners that are new to this domain, or the personnel that attend the MEL/MIL process or are part of an RC during a major exercise for the first time. All the information delivered through these papers provides a basic understanding of the exercise process and offers advice on how to improve support for exercises.

In an uncertain security environment that relies on the training quality of NATO and national troops to convey a message of unity and strength, coordination and synchronization of knowledge are essential. To properly support an exercise as part of the RCs, the requirements are very high. While being a Subject Matter Expert (SME) in your domain is crucial for the TA, it alone is not sufficient for RCs' personnel. As explained above, in addition to excelling in their respective roles, RC personnel should possess a comprehensive understanding of the exercise process and their role within it. The quality of the exercise depends on their level of training in this field. While NATO Bi-SCD 75-003 provides a detailed guideline for the 4 stages of the exercise process and is considered the exercises' planners' Bible, it may be challenging for those playing smaller roles in the exercise and not involved in all aspects of the planning process to fully grasp their role using this training directive. We hope that our research papers will support them.

BIBLIOGRAPHY:

1. Jacek Welz and Gultekin Arabaci. 2016. JCATS Introduction Course presented at Modeling and Simulation Centre of Excellence in Rome. (In-text citation: Jacek Welz and Gultekin Arabaci, 2016, 6).
2. NATO Exercise Process BI-STRATEGIC COMMAND DIRECTIVE 075-003. 2023. (In-text citation: Bi-SCD 75-3, 2023, Annex1, Appendix 2, A-2-5; Annex Z, Z-1-4; Annex F F-8)
3. Zinca Diana and Ghiță Bârsan. 2018. Constructive simulation programs and NATO Functional Area Services applied in Computer Assisted Exercises, Revista Academiei Forţelor Terestre Nr. 2 (90)/2018 (In-text citation: Zinca Diana and Ghiță Bârsan, 2018, 164)
4. Zinca Diana and Ghiță Bârsan. 2020. Main Events List/ Main Incidents List development process For Computer Assisted Exercises presented in International Conference Knowledge-Based Organization. Sibiu. Romania
5. Zinca-Emch Diana. 2023. M&S CAX Support Course presented during the Exercise Planning Process at Component Level Course at Rapid Reaction Corps France.(In-text citation: Zinca-Emch, 2023, 20).
6. www.sto.nato.int

1053477-3045-1396-24-13

DRONE WARS: TACTICAL IMPLICATIONS OF UAS EMPLOYMENT IN DIVISION-LEVEL WET-GAP CROSSING OPERATIONS

Petru – Marian VEREȘ, PhD. candidate
Romanian Army Major, PhD. candidate,
Superior Instructor at "Carol I" National Defense University, Bucharest, Romania
E-mail: verespetrumarian@gmail.com

Abstract: *The current Russian – Ukraine war revealed a new key capability that significantly changed land tactics and combined arms maneuver, shifting the odds of success in favor of the unit that employs it in a more effective way. Weaponized drones have been widely used in this conflict and there are many lessons to be learned, regarding their integration into army land tactics, their employment throughout the battlespace, and possible ways of countering their actions and effects. This research endeavor is constructed on a qualitative analysis of the data collected through content analysis and comparative analysis methods, and considers the implications of the employment of drones in wet-gap crossing operations, by focusing on how they affect land tactics and maneuver, in order to create a better understanding of the future battlespace and offer refined ways of employing drone equipped land tactical units.*

Key words: *weaponized drones, land tactics, combined arms maneuver, integration and employment, land operations, autonomous sensor, target engagement.*

Introduction

The overall field of this paper's subject is *military tactics,* more specifically *land tactics*, and it emphasizes the tactics adopted by division level units in wet-gap crossing operations. The problem this article addresses consists in identifying the implications that occur with the introduction of unmanned aerial vehicles in land tactics. Therefore, in order to create a better understanding of the identified implications, this article is built upon three chapters, addressing the study of various types of UAS and their employment in the Russo-Ukrainian War, the improvements and particularities that drones bring with their integration in division level wet-gap crossing operations, and the possible ways of adapting current wet-gap crossing tactics.

Background

Land forces units are employed across the battlespace in order to create effects and achieve the established objectives, according to a higher echelon's vision and concept. Land forces create effects through tactical actions and fire employment oriented against an enemy, while seeking to preserve combat power. However, land engagement is complex and often unpredictable, and various types of obstacles can impede the maneuver of land units, and serve as a strong point for a defending enemy. A weaker force will resort to a temporary defensive action, in order to create the necessary conditions for an offensive operation, and it has been proven throughout history that a wide natural flowing watercourse can be a perfect line of defense. A wide river, for example, generates a wide range of challenges for an attacking force, multiple opportunities for a defending force, and is therefore the preferred obstacle to establish a strong defensive line.

In the current Russo-Ukrainian War, after the Kiev offensive failed, the Russians retreated to the east, in order to establish a frontline, along their consolidated gains. During the autumn of 2022 and most of 2023, this established frontline was pushed forward by both sides, by means of a war of attrition, with no notable results other than large numbers of casualties. However, in the south of Ukraine, the Russian established frontline, along the Dnipro River between Herson and Zaporojie, was virtually an impenetrable defensive sector where little to no operations, other than fire employment, had been conducted by either side.

Even with the employment of technological advanced drones and other autonomous systems, the conduct of an offensive operation, across a river like the Dnipro, with the enemy in a well defended positions on the other bank, might be the most challenging land operation we can think of in Ukraine, requiring a multi-domain engagement of capabilities, thorough planning and risk tolerance.

Looking back in history, many great military campaigns have had river crossings as a crucial turning point to their overall success. Moreover, these types of operations have often constituted the moments when generals decided to stop and rethink their offensive plans or an obstacle they would use as a defensive line. One historical example of a challenging operation, as written in "Professional Memoirs, Corps of Engineers, United States Army, and Engineer Department at Large", a publication issued by The Society of American Military Engineers, was the crossing of the Danube River by the Russian army, during the 1877 Russo-Turkish War, when the Russians had halted for several weeks on the bank of the Danube, before they decided it was possible to venture the crossing, regardless of the poorly led and weak Turkish forces on the Bulgarian bank (Immanuel and Gotwals 1916, 509).

River crossings are the most difficult types of wet gap-crossing operations, involving extensive preparation and flexible planning, surprise and speed (FM 3-90/2023, 18-10). The introduction of drones into land tactics, as we can observe in the current Russo-Ukrainian war, cannot ensure success in a wet-gap crossing operation on its own, but surely facilitates the execution of tactical actions and can provide that crucial freedom of action that tactical units need while conducting such an operation.

Statement of the problem, the rationale behind the article and its significance

Military tactics has been the subject of many articles and publications and a wide variety of tactical implications of different capabilities has been researched by authors and organizations. Although the existing literature contains detailed analyses of the tactics involved in virtually every major conflict in modern history, specific details and the tactics behind wet-gap crossing operations can only be found in military doctrines and manuals. Moreover, the integration of drones in tactics, as well as the resulting implications, have not yet been covered by scientific researchers, and most tactical field manuals, especially US Army or Allied Publications, have not yet addressed this subject.

In order to ensure a proper start to this research approach, the author has formulated the following research problem: *Unmanned aerial vehicles have not yet been fully integrated into military land actions doctrine, leading to a gap in describing the implications that result from the employment of drones in division-level wet-gap crossing operations. Despite this, there is limited research aimed at establishing a baseline for land forces divisions to execute wet-gap crossing operations with the employment of drones. Therefore, this paper aims to determine the tactical implications of drone integration in wet-gap crossing operations, executed by combined arms divisions in conventional warfare*.

Military doctrines serve as guidelines for how soldiers fight and commanders lead so it is quite obvious why doctrines must cover every possible aspect regarding the use of the new technologies and capabilities that are integrated into armed conflict. Furthermore, given the fact that doctrines are mostly developed by integrating the results and demonstrated facts provided by scientific research, warfighting experience gained by soldiers on the battlefield and results obtained from testing, experiments and military applications, the results of a study on the tactical implications of drone employment during wet-gap crossing operations may constitute a much-needed start for the development or update of the military doctrine itself.

This research paper aims to explore the possible tactical implications of drone employment during the execution of wet-gap crossing operations, at division level. In order to achieve the established research aim, the following research objectives must be set:

1. Analyzing the technical and tactical capabilities of the current types of drones that are available for combat deployment, by February 2, 2024;
2. Identifying the effects that the analyzed drones can produce when employed in wet-gap crossing operations, by February 7, 2024;
3. Analyzing the impacts that the effects of drone employment have on the tactical actions that build up the wet-gap crossing operation, by February 11, 2024.

Given the formulated research objectives, the following research questions are needed as the driving force behind the research endeavor:

1. Which types of UASs are currently employed in an operational environment? What capabilities do they possess? Which are their technical and tactical characteristics? What are their inherent limitations?
2. Which actions compose a wet-gap crossing operation? How are they sequenced?
3. Which effects are needed in order to ensure a successful wet-gap crossing operation? How will the employed UASs contribute in the achievement of these effects?

This research project addresses the implications of drone integration in division-level land tactics, specifically deliberate wet-gap crossing operations and does not study the joint level of the operation. Moreover, the study is limited to the tactical aspect of those types of operations, addressing the tactical actions of the division as a combined arms force and does not address each divisional element separately.

This research paper is very important to the military science community for various reasons. Firstly, this paper constitutes a starting point from which the land forces doctrine developers may begin an update of the existing doctrines, with respect to the studied subject, or a component than can be used to build on the existing manuals or procedures. Secondly, the paper can offer a clearer understanding of what the UAS can provide the land forces with in an operation, and help military commanders with a common problem in todays' environment. Lastly, this study consolidates the observations and lessons learned from the conflicts where UASs are employed in a research paper that may offer a glimpse of what future conflicts may generally look like.

I. The Unmanned Aircraft Systems of today's conflicts

The UAS has had a constant presence in past and current conflicts, given its capability and facile employment on the battle space. The UAS is a versatile weapon, capable of executing combat, combat support or combat services support missions, throughout the battlespace.

Widely used and commonly known, the MQ-1 *Predator* UAV was first used in 1995 in the Balkans and has proven to be ideal for unmanned ground surveillance for the next decade. Predator drones were also used in Kosovo, in 1999 where they were used to locate enemy positions concealed in forests or towns, flying at low altitudes where manned aircraft would not have been safe from ground fire. During the War in Afghanistan, the Predator UAV was used by the CIA (Central Intelligence Agency) to locate Osama Bin-Laden and the agency later began arming its Predators and using them to conduct additional strikes against suspected al Qaeda and Taliban leaders in Afghanistan (Walsh, Schulzke 2018, 11-13). Additionally, the Predator drone was used to conduct strike missions in Afghanistan, executing a modest number of missions, using mostly AGM-114 Hellfire missiles. The Predator was initially built as a surveillance drone but, due to its technical characteristics (see Table no. 1) it has proven itself as a very efficient striking capability.

After the withdrawal of Coalition forces from Afghanistan, the Russian invasion and military operations in Ukraine began. In February 2022, the Russian Armed forces began a major military operation to capture the capital, known as *The Battle of Kyiv*, and began advancing towards the city from the North, on 3 major axes: Chernobyl, Chernihiv and Sumy. During their advance, the Russian columns had to make their way around cities; on narrow forest roads their personnel, vehicles, arms, and equipment became easy targets for Ukrainian mobile groups. Videos shot in the area showed columns of Russian tanks burned by artillery fire, drones, and lightly armed Ukrainian mobile groups (Plokhy 2023, 159).

The main type of UAS used during the first stages of the Russo-Ukrainian War was the Bayraktar TB2, a Turkish system that executes both strike and ISR (Intelligence, Surveillance and Reconnaissance) missions. Due to its superior features (see Table no. 1), the Bayraktar UAS has become an essential weapon in this war and prompted the Russians to quickly update the way they think and execute air defense operations. On the other hand, the successful missions and the good results that the employment of drones had brought, the Ukrainians began developing an entire warfighting concept around these systems, making them ever present in their actions. In an excellent study by The Royal United Services Institute, materialized in the publication called *"Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022"*, Mykhaylo Zabrodskyi revealed that a key lesson from the war is that UAS and CUAS must be available at all branches of the force. Moreover, Zabrodskyi stated that UAS should be split into three broad categories for land forces: "*rotary-type UAS … able to maneuver close to the ground and in complex terrain for the purposes of route proving, reconnaissance, situational awareness, target acquisition, fire correction, and a wide range of other tasks; fixed-wing UAS able to fly at medium altitude into operational depth and perform a single task, whether that be target acquisition or direct effects; … and platforms carrying higher echelon sensors … including the TB2"* (Zabrodskyi and others 2022, 58).

Building upon this concept, the Armed Forces of Ukraine developed a framework of drone employment orientated towards target detection and engagement. This means that they organized their capabilities to optimize drone employment, to find the targets, strike and then assess the damage and effects. During an official visit in Romania, major general Ihor Palahniuk, the acting Land Forces Commander of the Armed Forces of Ukraine, detailed this framework during the workshop organized by the Romanian Land Forces Command. According to major general Palahniuk, the largest tactical Ukrainian Land Forces unit is the brigade, held under the command of a tailored land task-force and tactical-group headquarters. If we compare this command-and-control system with a NATO Land Force one, the Ukrainian task-force would be the equivalent of a land force corps command and the tactical-group a division level command. At the operational level, the Ukrainians organized Joint Force Commands, and the Khortytsia, Tavria and Odesa are good examples, which subordinate the task-forces.

In contrast, each UAS capability is held under the command of an HQ, depending primarily on the effects they can produce, their operational reach and their technical features. Thus, the operational level drones they employed are the PD-1 *People's Drone* (UkrSpecSystems 2024) reconnaissance drone, the PD-2 multi-purpose (reconnaissance and attack) drone and the *Ray Bird* (Skyeton 2024) reconnaissance drone. The Ukrainian Brigades and Tactical-Groups employ the *Leleka 100* reconnaissance drone (UkrSpecSystems 2024), the A1-CM *Furia* reconnaissance drone (Athlonavia 2024), the *Vector* ISR drone (Quantum-Systems 2024), the *Shark* reconnaissance and fire adjustment drone (UkrSpecSystems 2024) and the *Fly Eye* reconnaissance and fire adjustment drone (WBGroup 2024).

The battalions and smaller tactical formations mostly employ quadcopter UAVs, with reduced range and flight duration, but capable of dropping small explosive devices on personnel and light armored vehicles as well as conducting fire adjustment, surveillance and reconnaissance tasks. These types of drones are not built for ISR and striking missions by their manufacturers, but the Ukrainians managed to weaponize and employ them to find and strike Russian positions and vehicles. Some examples of weaponized commercial drones used in Ukraine are the DJI Mavic and Matrice drones and the AutelEvo reconnaissance drone.

Russians and Ukrainians have managed to integrate loitering munitions within their tactics. Brennan Deveraux characterized, in an article posted on the *War on the Rocks* on-line platform, loitering munitions as "*one-time-use weapons designed to find a target and crash into it, giving it its "kamikaze" nickname*" (Deveraux 2022). The Ukrainian preferred loitering munition was the *RAM II* drone (RAMUAV 2024), which was significantly less competent than the Russian employed *Shahed-136,* in terms of range, flight time or payload capacity (see Table no. 1 for details). While these types of weapons come in handy at some point during an engagement, they lack the capacity to produce critical effects over enemy actions. Still, they can disrupt enemy operations, in certain moments and over limited periods of time by striking elements of infrastructure or capabilities, such as battlefield sensors, communications systems, power generators, and other elements needed to ensure survivability, force protection or intelligence collection. Loitering munitions' successful actions depend largely on the level of produced intelligence, the ability to evade radar detection and the employing unit's capacity to launch multiple munitions at once (Kunertova 2023, 98).

Table no. 1. *UAS capabilities and technical features* (created by the author)

Types of UAS employed by the Ukrainian Armed Forces and their features and technical characteristics			
MQ-1B Predator - type: multi-purpose; - range: 1240 km; - payload: 204 kg; - speed: 215 km/h; - ceiling: 7620 m.	**Bayraktar TB2** - type: multi-purpose; - range: 27 h of flight time; - payload: 150 kg; - speed: 220 km/h; - ceiling: 5400-7600 m.	**Vector** - type: reconnaissance; - range: 180 km; - payload: N/A; - speed: 80 km/h; - flight time: 180 min.	**PD-2** - type: multi-purpose; - range: 1300 km; - payload: 11 kg; - speed: 140 km/h; - ceiling: 4700 m.
Ray Bird 3 - type: reconnaissance; - range: 2500 km; - payload: N/A; - speed: 140 km/h; - ceiling: 4500 m.	**A1 CM Furia** - type: reconnaissance; - range: 50 km; - payload: N/A; - speed: 65 km/h; - ceiling: 1200 m.	**RAM II** - type: loitering munition; - range: 30 km; - payload: 3 kg; - flight time: 55 min; - ceiling: less than 1000 m.	**Shark** - type: reconnaissance; - range: 300 km; - payload: N/A; - speed: 130 km/h; - ceiling: 3000 m.

Fly Eye	**Leleka**	**DJI Mavic**	**AutelEvo**
- type: reconnaissance; - range: 30 km; - payload: N/A; - speed: 120 km/h; - ceiling: 4000 m.	- type: reconnaissance; - range: 100 km; - payload: N/A; - speed: 70 km/h; - ceiling: 1500 m.	- type: multi-purpose; - range: 21 min flight time; - payload: 500g – 2 kg; - speed: 64 km/h; - ceiling: max. 1000 m.	- type: multi-purpose; - range: 40 min flight time; - payload: 500g – 700 kg; - speed: 70 km/h; - ceiling: max. 7000 m.

During all tactical operations, the UAS are not employed randomly, but are integrated in a coherent manner into the tactical actions. Moreover, the information gathered by these capabilities must be processed and developed into intelligence, and disseminated to the operators; so constant communication with the operator is a must. Furthermore, as we stated earlier, drones are employed at different echelons throughout the area of operations.

A division area of operations is large, spanning up to 130 km from its rear area to its deep area, where a division's effects end (FM 3-0/2022, 6-8). Therefore, given their characteristics and technical capability, drones are employed in the rear, close and deep areas. While the rear area of a division is less likely to have the need for drone capability employment, the close and deep area is where the effects of drones is most required. Ukrainians employ drones by means of battalion and lower echelons in the close areas (usually DJI Mavic 3 or AutelEvo), by means of a brigade in the tactical deep area, as far as 30 km from the contact line (FlyEye and Shark drones for reconnaissance and Leleka, Furia or kamikaze drones such as RAM II, for strike missions), and further into the operational deep (PD 1 and 2 or Ray Bird type drones). This important task requires a robust communications and information system, capable of round the clock battlespace monitoring, maintaining constant communication with drone operators and junior commanders as well as constant situational awareness.

Like all systems, UAS come with limitations and vulnerabilities. Typically, a UAS is composed out of 3 elements: the unmanned aerial vehicle (UAV), the ground control station and the communication data-link (Yaacoub & others 2020). Weaponized drones also have an improvised or added component, the payload or munition attached to it. The UAS construction features and their employment requirements generate various vulnerabilities and limitations:

- enemy air defense capabilities: drones are small unarmored vehicles with little to no countermeasures against enemy air defense. Their ability to remain undetected remains their only defense and this depends largely on the enemy's detection and counter asset availability;
- enemy electronic warfare engagement: UAS can be hacked, leading to their data manipulation, alteration of flight paths, redirection of payload delivery or crash induction;
- malfunctions and other technical failures may render an UAS incapable of accomplishing its mission;
- UAS are fairly complicated and operating them can often be a challenging task for an unskilled operator. The incorrect use of the system coupled with human error may lead to drone crashes and other forms of system malfunction;
- UAS use airspace as an operational domain so weather challenges often occur. Strong wind, storms, fog, temperature and humidity can disrupt drone functions and cause malfunctions.

Additionally, as major general Palahniuk pointed out during his presentation of the Armed Forces of Ukraine's performance in the Russo-Ukrainian War, drones that carry payloads, FPV (First Person View) drones or loitering munitions can miss their targets, can explode during their flight or their payload may not explode upon impact.

Drones bring substantial advantages through their capabilities and technical features, but not without limitations. Taking the first chapter's findings into account, we can assume that the way of employing UAS in warfighting is strongly influenced by correct timings, the available systems, the number of drones a military unit possesses and the environmental factors. As doctor James Rogers and Dominika Kunertova so accurately revealed in their relevant report, "*drones will be deployed in ever greater multiples of 10s, 20s, or potentially 100s as they are sent as part of multidrone and missile launches towards military, industrial, or civil targets in an attempt to saturate and overwhelm available air defence systems*" (Rogers & Kunertova 2022). Moreover, a strong emphasis must be put on operator training and the technological development of the systems.

II. Tactical implications of drone employment in wet-gap crossing operations

The US military doctrine considers the land force division as a principal tactical warfighting formation during large-scale combat operations (FM 3-94/2021, 5-1). Given its nature, a division conducts large-scale operations by employing various types of units and capabilities in a combined arms manner. The same military doctrine states that normally, the division is the smallest tactical unit that can execute wet-gap crossing operations during large-scale operations (FM 3-90/2023, 18-14). Rivers are usually the preferred obstacles for a defending force, to organize a strong defensive position, therefore they also constitute a difficult challenge for an attacking force.

A wet-gap, specifically a river-crossing operation, usually requires extensive planning, preparations and rehearsals, detailed reconnaissance and plans to coordinate fires. Multiple engineer assets are also a critical requirement, as they are essential for crossing the troops and capabilities from one side of the river across to the other. Moreover, an operation this complicated requires a higher echelon to coordinate the different actions and activities that are conducted by subordinate units.

As we stated during the first chapter of this paper, depending on their mission requirements and technical capabilities, UAS are held at and employed by different tactical echelons, each having a precise role within the overall design of the operation, therefore, a needed tenet for drone employment would be the covering of the entire area of operations. This is not an easy task for a conventionally built tactical unit but with the integration of UAS capabilities, the rear, close and deep areas (FM 3-0/2022, 6-8) of the division area of operations are ever so accessible.

According to the US army tactics field manual *F.M. 3-90 Tactics,* a deliberate wet-gap crossing, as part of a larger offensive operations, needs a special organization of forces: an assault force, assured mobility forces, a bridgehead force and breakout forces. Each of these force groups need UAS support to accomplish their tasks and their actions are phased. Normally, according to the same US military tactics doctrine, F.M. 3-90, a deliberate wet-gap crossing operation has 5 phases.

In the first phase, the division seeks to set the conditions for a successful crossing. During this phase, the division employs fires to strike enemy targets in the close and deep area. This phase is particularly important because it may shape the environment in such a way, that the crossing operation's success can depend solely on it. Destroying the enemy combat power, delaying its supply lines and disrupting its intelligence and communications capabilities can lead to breaking the will to fight or may cause retreat.

During this phase, division artillery elements, based on their range, engage targets located across the close and deep area. This action aims to ensure an efficient start for the attack sequences and freedom of action for the subordinate brigades, as they begin their movement from rearward assembly areas to forward attack positions, located near the crossing points (ATP 3-91/2014, 6-7). Reconnaissance units are also sent forward to the nearside objectives to locate the favorable crossing sites.

This phase requires efficient strike operations, substantial reconnaissance and unobstructed mobility for the subordinate brigades. The division needs to fight the deep to ensure close area operations, as far as their range can allow. Modern NATO divisions employ capable long range MLRS such as HIMARS, with an effective range as far as 130 km (ArmyRecognition.com, 2022). Fire correction at that distance may be easily ensured with the employment of a fast, high-altitude reconnaissance drone like the *Shark* UAS. Furthermore, strike operations in the deep areas are challenged by the constant movement and repositioning of the targets so missile strikes may often prove inefficient. A multi-purpose drone like the *Predator*, the *Bayraktar* or *PD 2* can engage both static and mobile targets, to disrupt or neutralize enemy C2 and sustainment operations, engage artillery systems, air defense capabilities or enemy important infrastructure elements.

In the close area, to ensure timely information, all types of reconnaissance drones may be employed with ease and UAS like the Vector can survey the nearside objectives and crossing points for hours. Additionally, the small and stealthy *DJI Mavric* and *AutelEvo* quadcopters can strike fortified defensive positions, soldiers dug in trenches, to spoil enemy defensive actions on the other bank, and destroy armored vehicles that are otherwise hard to engage during this phase of the operation.

The second phase of the wet-gap crossing operation, according to FM 3-90, is the advance to the gap phase. In this phase, the division employs the subordinate brigades to engage the enemy elements and seize objectives, in order to secure nearside terrain which offers favorable crossing sites and road networks and provide enough area to stage crossing forces (see Figure number 1).

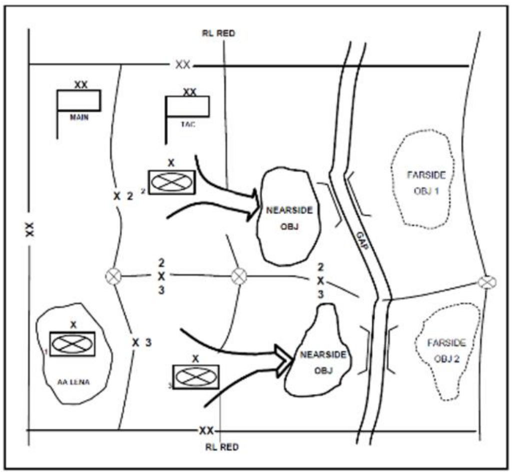


Figure no. 1. Advance to the gap (FM 3-90.12/2008, 4-15)

UAS may support the actions of the division by ensuring constant reconnaissance over the close area, particularly over the nearside key terrain and the enemy actions, while continuously engaging targets in the enemy deep. Attacking enemy positions requires combined arms maneuver and fires, so drones, as we can deduce, can be integrated as an addition amongst the arms and services, to strengthen the fundamental principle of combined arms warfare which, as written in ADP 3-0 Operations, relevantly states that engaging one capability makes the enemy vulnerable to another (ADP 3-0/2019, 3-9).

During the third phase of the operation, the division aims to attack enemy defensive positions on the other gap side, in order to ensure the far side objective. This is also done to eliminate direct fire assets that may engage division forces while they cross. This action is by far the most challenging because it requires brigades to cross the river, by any means possible, assault and defeat enemy positions, while constantly under indirect fire form the enemy deep.

This is the phase when loss of life and capability destruction is the heaviest so finding a way to preserve combat power is a must.

At this phase, strike UAS, especially FPV kamikaze drones and quadcopters, are most effective. These types of drones, when engaged as a swarm, may cause crucial damage to enemy positions and direct fire capabilities, C2 systems and ISR capabilities. While artillery and other means of indirect fire are severely limited beyond the exit bank during this phase, due to the gap splitting the attacking force, strike drones like the *Bayraktar* or *PD 2* can compensate. While these drones act, dismounted infantry and amphibious armored vehicles have more freedom of action and are able to maintain a fast tempo and a fast crossing of the gap. Drones also impose dilemmas for the enemy, that may have to decide which effort to engage first, the drones or the soldiers crossing the river. Additionally, the employment of drones during this phase, in contrast to indirect artillery fire employment, reduces the risk of fratricide and facilitates airspace management.

In the fourth phase of the operation, after seizing the far side objectives, the subordinate brigades attack and seize objectives further, in order to clear the area of enemy direct and indirect fire capabilities. This action ensures freedom of action, protection and time for the other division units to develop the crossing sites, by constructing rafts or bridges, and to ensure the crossing of heavy division units. Ultimately the buildup of forces in the far side objectives is needed in order to ensure a continuation of the larger offensive operation towards the intermediate objective (See figure number 2).

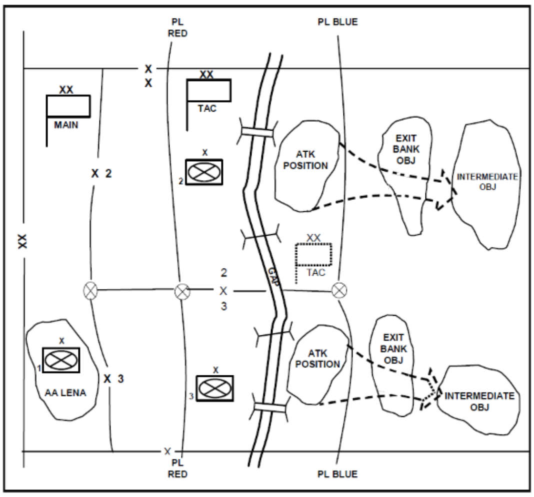


Figure no. 2. Advance from the far side (FM 3-90.12/2008, 4-18)

During this phase, UAS must be employed further into the deep as the area of operations extends. The multi-purpose drones must identify and strike at enemy reserves and long-range indirect fire assets. Moreover, drones must engage sustainment units and assets to prevent the resupply of enemy troops in the close area.

The next phase of the operation begins with an assault from the conquered intermediate objectives, to secure a bridgehead line by occupying objectives in key positions, where the subordinate brigades organize a hasty defense. Securing this bridgehead line is crucial for the success of the overall offensive operation for two reasons. Firstly, it ensures that the combat support and services cross the river and place themselves in the division battle disposition, in order to ensure timely support for the defending brigades. Secondly, it ensures a protected preparation for a break-out force to continue the offensive operation from the bridgehead onward.

To successfully hold the bridgehead line, the division has to ensure the continuous prevention of spoiling attacks, infiltrations or strike missions, that would definitely hinder the river crossing effort for the rest of the division units. This implies the extensive battle field reconnaissance, especially for the flanks and execute deep operations and strike missions on enemy counterattack forces.

The defending brigades need sufficient combat power to be able to control avenues of approach and defeat counterattack units so, preserving their soldiers and capabilities is crucial. This can be done by employing reconnaissance drones to screen the flanks constantly, and double the effort of the ISR units, and in the same time, conduct deep strike operations with multi-purpose drones that strike at enemy counterattack units as well as correct fires for the division indirect fire missions. Time is crucial for the break-out force's attack, which needs to be done as soon as possible, so gaining time by employing drones is absolutely necessary. The continuation of the attack by the break-out force is the last phase of the operation, and the success of this task is also ensured by rapid employment of UAS, to strike high value targets and constantly supply the division C2 with timely information and fire correction.

Conclusions

The conclusions of this research paper will summarize the key research findings in relation to the research aims and questions stated in the introduction, and discussing the value and contribution thereof. It will also review the limitations of the study and propose opportunities for future research.

This study aimed to explore the tactical implications of UAS employment during a division's wet-gap crossing operation. The results point out that employing drones in this type of operation will change the tactics of this type of operation, to a limited extent, but will not change the phases or sequencing required for execution. Further findings indicate that drone employment can make the enemy deep area more accessible, by the provision of information, fire correction and key target engagement. Moreover, the actions of the maneuver brigades could be supported by UAS employment through combined arms engagement of enemy defensive positions which might lead to the creation of multiple dilemmas for the enemy. Drones can increase the accuracy of the attack by fire against dug-in defensive positions and can enhance the unit's capability to destroy armored vehicles. Also, the correct and efficient employment of drones can lead to the disruption the enemy's ability to strike the crossing units, by striking the ISTAR capabilities, C2 nodes and other crucial infrastructure elements that the enemy uses.

The results obtained through this research paper point out the necessity for the development of gap-crossing military doctrines and field manuals, which integrate drones as a tactics changing capability, and new ways of organizing tactical units, establishing minimum essential control measures and general planning, preparation and execution considerations, in order to ensure a coherent UAS integration. Furthermore, testing UAS capabilities in accordance with the research paper's results and findings during military exercises, might reveal new frameworks and insight for military commanders, contributing to the evolution of military tactics on par with the current operational environment.

The limitations of this study mainly consist in the reduced access to we-gap crossing operations doctrines. The tactics studied are mainly extracted from the US military doctrine and the results obtained are not necessarily general. The results obtained might be applicable to NATO member countries, which follow the same tactical standards. It is worth, however mentioning that this limitation occurs not from a research bias towards US tactics, but from a lack of access to other military tactics doctrines, due to their restricted public release. Moreover, most of the results of this research are only sustained by limited research regarding UAS employment in the Russo-Ukrainian War of 2022. Many aspects regarding drone employment in military operations have yet to be researched and a significant gap in scientific research on this topic still exists.

Considering these limitations, future research projects on this topic, or related topics for that matter, should follow a more complex research method, in order to enhance the generalizability of the findings and collect data from more resources. Continuing the research on UAS employment in military operations and in the inherent tactical implications might prove to be extremely important for future wars because these capabilities might shift the military thinking towards shortening combat operations and consequently reducing the loss of lives and infrastructure destruction.

UAS employment in military operations is a thing of the future and we need to reveal, in a scientific manner, that the way military commanders choose to employ these capabilities depends largely on the way we advise them to do so.

BIBLIOGRAPHY:

1. Immanuel, Friedrich. Gotwals, John C. "*Professional Memoirs, Corps of Engineers, United States Army, and Engineer Department at Large*". Published by The Society of American Military Engineers. USA. July-August, 1916, Vol. 8, https://www.jstor.org/stable/44698065
2. *Field Manual 3-90 Tactics.* Headquarters, Department of The Army. USA. Washington D.C. 1 May 2023.
3. Walsh, James Igoe. Schulzke, Marcus. "*Drones and Support for the Use of Force*". University of Michigan Press. Ann Arbor, USA. November 2018.
4. Plokhy, Serhii. *"The Russo – Ukrainian War. The Return of History".* Published by W. W. Norton & Company, Inc., New York, SUA, 2023.
5. Zabrodskyi, Mykhaylo, Watling, Jack, Danylyuk, Oleksandr, Reynolds, Nick. 2022. "*Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022*", Royal United Services Institute for Defence and Security Studies, London, November 2022.
6. UkrSpecSystems 2024. "PD-1 Unmanned Aerial System". Accessed February 13, 2024. https://ukrspecsystems.com/drones/pd-1-vtol
7. Skyeton 2024. "*Ray Bird 3*". Accessed February 13, 2024. https://skyeton.com/ en/raybird/
8. UkrSpecSystems 2024. "*Leleka 100*". Accessed February 13, 2024. https://ukrspecsystems.com/drones/leleka-100-electric-uav
9. Athlonavia 2024. *"A1-CM Furia".* Accessed February 13, 2024. https://athlonavia.com/en/furia/
10. Quantum-Systems 2024. "*Vector*". Accessed February 13, 2024. https://quantum-systems.com/vector/
11. UkrSpecSystems 2024. "*Shark*". Accessed February 13, 2024. https://ukrspecsystems.com/drones/shark-uas
12. Wbgroup 2024. "*Fly Eye*". Accessed February 13, 2024. https://www.wbgroup.pl/en/produkt/flyeye-unmanned-aerial-system/
13. Deveraux, Brennan. "*Loitering Munitions in Ukraine and Beyond*". War on the Rocks platform. April 2022. https://warontherocks.com/2022/04/loitering-munitions-in-ukraine-andbeyond/
14. Kunertova, Dominika. *"The war in Ukraine shows the game-changing effect of drones depends on the game".* Published in the Bulletin of the Atomic Scientists no. 79, Vol. 2. 2023.
15. *Field Manual 3-0 Operations.* Headquarters, Department of The Army. USA. Washington D.C. October 2022.

16. Yaacoub, Jean-Paul. Noura, Hassan. Salman, Ola. Chehab, Ali. “*Security analysis of drones systems: Attacks, limitations, and recommendations*”. Published in The Internet of Things Journal. Beirut, Lebanon. May 8, 2020. https://www.sciencedirect.com/science/article/pii/S2542660519302112?via%3Dihub#bib0003
17. Rogers, James. Kunertova, Dominika. “*The Vulnerabilities of the Drone Age Established Threats and Emerging Issues out to 2035*”. Final report for The Center for War Studies. The NATO Science for Peace and Security Programme. 2022.
18. *Field Manual 3-94 Armies, corps and division operations.* Headquarters, Department of The Army. USA. Washington D.C. October 2022.
19. *Army Techniques Publication 3-91 Division Operations.* Headquarters, Department of The Army. USA. Washington D.C. October 2014.
20. Armyrecognition 2022. “*Analysis: M270A1 IAC and M142 HIMARS are able to fire a wide range of rockets and missiles*”. Accessed February 15, 2024. https://armyrecognition.com/weapons_defence_industry_military_technology_uk/analysis_m270a1_iac_and_m142_himars_are_able_to_fire_a_wide_range_of_rockets_and_missiles.html?utm_content=cmp-true
21. *Army Techniques Publication 3-90.12 Gap Crossing Operations.* Headquarters, Department of The Army. USA. Washington D.C. July 2008.
22. *Army Doctrine Publication 3-0 Operations.* Headquarters, Department of The Army. USA. Washington D.C. July 2019.

1053477-3045-1396-24-14

MAPPING DATA SHOES' IMPACT ON THE BATTLEFIELD: EXPLORING CHALLENGES AND CONSIDERATIONS FOR TACTICAL LEVEL SUB-UNIT TRAINING WITH MULTIPLE INTEGRATED LASER ENGAGEMENT SYSTEMS IN MODELING AND SIMULATION

Claudiu Dumitru VESA
LTC, PhD. student at "Carol I" National Defence University, „Nicolae Bălcescu"
Land Forces Academy of Sibiu, Sibiu, Romania
E-mail: vesa.claudiu@armyacademy.ro

Adina Nicoleta STRIAN
PhD. student at "Lucian Blaga" University of Sibiu, „Nicolae Bălcescu"
Land Forces Academy of Sibiu, Sibiu, Romania
E-mail: strian.adina@armyacademy.ro

Abstract: *Current studies emphasize the importance of accurate measurement of foot pressure distribution in identifying and treating the root causes of biomechanical problems. Against this backdrop, the use of an integrated footwear system, such as tactical footwear, becomes essential for the prevention of some conditions and for the effective management of effort, leading to the reduction of fatigue and blood pressure and consequently to the improvement of physical endurance on the battlefield. The present study aims to investigate the mapping of data regarding ultra-thin footwear force and pressure and their impact on influencing movement in the military environment. We have analysed the gait of 30 military students using the F-Scan64, a wireless in-shoe system equipped with micro-sized electronics. The results highlight the importance of data analysis of movement and weight distribution in order to better identify the risk factors and facilitate the implementation of preventive measures. Consequently, instructors will be able to accurately assess individual performance, thereby enhancing the effectiveness of tactical training.*

Keywords*: gait analysis, pressure distribution, patient database, military boots, biomechanics*

Introduction

Current studies emphasize the importance of accurate measurement of foot pressure distribution in identifying and treating root causes of biomechanical problems. Biomechanics is that branch of biology applied to sports to study physical exercise and endurance. Human biomechanics studies human movement, through the prism of anatomy, biomechanics, movement therapy (kinetotherapy), and physiology, the knowledge focusing on the individual who wants to either recover some skills or motor functions or to acquire some motor performance. Thus, biomechanics has applications both in the medical and physical recovery fields, as well as in the sports field, for testing and improving motor qualities (Budescu E., 2013, 3). From this point of view, the use of an integrated system in footwear, such as tactical footwear, becomes essential for the prevention of certain conditions and for the effective management of effort, which leads to the reduction of blood pressure and fatigue and, therefore, to the improvement of physical endurance on the battlefield.

In light of the rapid changes in the field of technology and the continuous evolution of the global environment, the exploration of new and insufficiently researched fields becomes crucial for the advancement of knowledge and for addressing contemporary problems. Against this backdrop, the analysis of the impact of the pressure exerted by the weight of the soldier and individual weapons and equipment on the sole of the foot in military footwear on the performance and health of soldiers, in military actions at the tactical level and in the training process, is a relatively unexplored and particularly important field. In a world characterized by various conflicts and military operations, where every detail counts, the importance of mapping and understanding the pressure exerted in footwear on the feet of military personnel becomes obvious. However, research in this area is limited, and few studies address this topic in a comprehensive and systematic way.

Thus, the present study aims to fill this knowledge gap by investigating and analysing in detail the impact of lower limb pressure in military footwear on military movement and performance on the battlefield. We aim to shed light on this topic by providing relevant empirical data and interpretations that facilitate a better understanding of how pressure and force exerted by footwear can influence the health and effectiveness of military personnel in various operational contexts. By using modern pressure mapping and data analysis techniques, we intend to make a significant contribution to the thorough understanding of this crucial aspect of military training. In addition, our interdisciplinary approach, which integrates knowledge from biomechanics, technology, and the military domain, will bring a complete and innovative perspective on the problem.

Furthermore, it is critical to emphasize the importance of training tactical subunits in the use of multiple laser engagement systems integrated into modelling and simulation in order to meet modern battlefield challenges. In this context, the MILES (Multiple Integrated Laser Engagement System) systems have become a crucial tool for the military, providing significant opportunities for realistic and effective training. MILES is a training system that provides military personnel with a realistic combat environment for training exercises. MILES provides tactical simulation through laser transmitters attached to each individual involved in the training activities. MILES training is proven to increase combat readiness and effectiveness (Federation of American Scientists, 1999). In addition, the analysis presented in this article highlights the importance and necessity of continuous monitoring of students during these training exercises, with the help of MILES systems, to ensure the constant development and improvement of their skills in realistic and relevant conditions.

All in all, by exploring this new and unexplored topic, we want to contribute to improving the training and health of the military, thus increasing the effectiveness and safety of tactical-level military operations in current and future contexts.

1. AIM of the paper

The present study aims to investigate the relative importance of mapping force and pressure data from military footwear in influencing movement, reaction, and action in the military environment. We analysed the gait of 30 military students using the F-Scan64, a wireless shoe-embedded system equipped with microelectronics. The results highlight that the analysis of movement and weight distribution data can significantly contribute to the identification of risk factors and the implementation of preventive measures to reduce the likelihood of injury among military personnel. This gives instructors the ability to accurately assess the individual performance of military students in various exercises and tasks, thereby increasing the overall effectiveness of the training process.

By determining the optimal level of pressure exerted on the lower limbs, at the level of the sole of the foot, in military boots, the research intends to improve the mobility and performance of the military by increasing safety, allowing them to adapt more effectively to the variability of the terrain and to the specific demands of the missions. By monitoring and adjusting the pressure on the foot in the boots, the research results will be aimed at improving comfort and minimizing fatigue, implicitly contributing to the overall well-being of military personnel.

2. Current stage of research

According to the F-Scan64 Manual (Tekscan, n.d.), foot pressure measurement can be used in real clinical settings for gait and biomechanics analysis, pre- and post-treatment assessment, ulcer prevention, sports medicine and rehabilitation, and confirmation of orthotic prescription. Consequently, by identifying how the pressure is distributed, we can identify biomechanical problems.

In the civilian environment, the specialized literature contains a series of papers that investigate F-Scan sensors, most of which are used in various specialized clinics that are part of the medical field for diagnosis, monitoring, and treatment of various ailments of the lower limbs. The research targets the performance of patients and identifies methods to prevent certain limb injuries or ailments, in the different categories of subjects, according to age, weight, activity, and other defining criteria. An important factor in exerting pressure on the legs is given by the stiffness of the military boot (Böhm H., Hösl M., 2010, 2467-2472), and, according to a study by Cikajlo and Matjacić, military boots with increased stiffness decrease the ankle joint by 33%, negatively altering walking speed as well as walking stability, especially on uneven surfaces, such as the battlefield (Cikajlo I, Matjacić Z.,2007).

Research in the field has demonstrated that various mechanical and design characteristics of military footwear can influence ground reaction force attenuation capabilities and ankle joint loading when the foot/ankle complex is forced into inversion. (J.D. Simpson, H. DeBusk, C. Hill, A. Knight, H. Chander, 2018, 53-57).

In the current research, it is important not only to bring new data to the area of pressure mapping on the lower limbs, at the level of the sole of the foot in military footwear, but also to reinterpret and develop existing ideas in this area. Human biomechanics and gait studies have been long-standing research topics, but their application in a military context is relatively new and undeveloped.

Specialized literature already records work that addresses aspects of walking and pressure distribution in different contexts, such as medical or sports. However, the application of this knowledge in the military field requires specific reinterpretation and adaptation, given the unique characteristics and requirements of military operations.

Therefore, this research's main purpose is to bring a new and innovative perspective on how the pressure exerted on the foot in military footwear can influence the performance and health of soldiers in combat environments. We have built on the foundations already established in human biomechanics and intend to expand and apply them in a way that is specific and relevant to military needs and requirements.

Thus, by reinterpreting and expanding old ideas in this field, we will contribute to the development of a deeper and more comprehensive understanding of the impact of military footwear on military performance and health, opening new directions for research and innovation in this field.

3. Materials and methods

30 military students participated in this investigation. They wore military boots equipped with pressure sensors and equipment for monitoring and analysing data. The information collected included data on the distribution of the pressure exerted on the lower limbs, at the level of the sole of the foot, in the military footwear, during the movement; the frequency of the steps; the level of comfort and any discomfort felt by the participants.

In the first phase, F-Scan 64 sensors were needed (see Figure no. 1), which are devices for monitoring gait and the pressure exerted on the lower limbs. They are ideal for natural gait analysis and communicate via Bluetooth without requiring cables that limit the subjects' mobility. F-Scan 64 sensors are part of the category of pressure mapping systems in shoes. With a scan rate of up to

100 Hz, data is easily received and can be collected and interpreted in less than three minutes. The sensors can be used for multiple scans and come in different sizes to accommodate a variety of subjects.

Figure no. 1. F-Scan 64 pressure sensors
(Source: Authors)

For the integration of the work in the military field we needed to find a method to apply the sensors in the tactical boots of the military students that are more robust and taller than the usual street sneakers existing on the market (see Figure no. 2).

Figure no. 2. F-Scan 64 pressure sensors applied on military boots
(Source: Authors)

To carry out the tests, we chose subjects aged between 20 and 24 years, 22 males and 8 females, with different body weights and heights. They were equipped with military boots with pressure sensors, facilitating the collection of data that was later centralized.

The investigation had a total duration of 240 hours (during the training of fighter skills, a stage included in the calendar of the cadets' activities) and was carried out in the training range of the Land Forces Academy, in Sibiu. Data accuracy was ensured by using calibrated pressure sensors and standardized data collection procedures. The personnel involved in data collection were military students with qualifications and special training (advanced knowledge of tactics and procedures applicable in military actions) to standardize data collection and verify their accuracy. The units in the sample were randomly selected from a population of available military students, belonging to the Land Forces Academy of Sibiu. The collected data were analysed using statistical methods and calculation procedures relevant to the objectives of the investigation. These aspects were rigorously managed to ensure the quality and validity of the results obtained in the investigation.

A graphics station HP VR Backpack G2, a computer with high technical characteristics with connected sensors for data interpretation with the help of the predefined software F-Scan 64 and the MILES system (Multiple Integrated Laser Engagement System) for the permanent monitoring of military students, was used. Due to the high mobility and connection with interchangeable external batteries, this station can easily be integrated into the tactical field (see Figure no. 3).

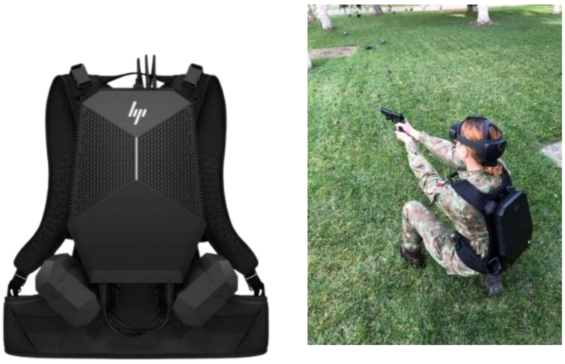
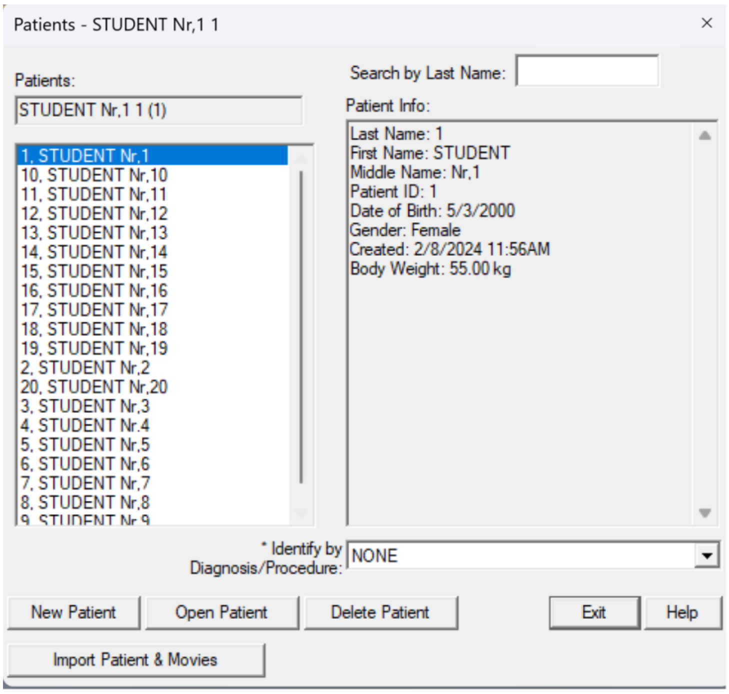


Figure no. 3. Graphics station HP VR Backpack G2
(Source: Authors)

4. Results

A table with the 30 military students participating in the test was created, containing their data: name, surname, weight, and sex. Also, individual IDs were assigned to each participant (see Figure No. 4).



Patients - STUDENT Nr,1 1

Search by Last Name:

Patients: STUDENT Nr,1 1 (1)

1, STUDENT Nr,1
10, STUDENT Nr,10
11, STUDENT Nr,11
12, STUDENT Nr,12
13, STUDENT Nr,13
14, STUDENT Nr,14
15, STUDENT Nr,15
16, STUDENT Nr,16
17, STUDENT Nr,17
18, STUDENT Nr,18
19, STUDENT Nr,19
2, STUDENT Nr,2
20, STUDENT Nr,20
3, STUDENT Nr,3
4, STUDENT Nr,4
5, STUDENT Nr,5
6, STUDENT Nr,6
7, STUDENT Nr,7
8, STUDENT Nr,8
9, STUDENT Nr,9

Patient Info:
Last Name: 1
First Name: STUDENT
Middle Name: Nr,1
Patient ID: 1
Date of Birth: 5/3/2000
Gender: Female
Created: 2/8/2024 11:56AM
Body Weight: 55.00 kg

* Identify by Diagnosis/Procedure: NONE

Figure no. 4. Test participants table
(Source: Authors)

Each student participating in the test was combat-equipped, and pressure sensors were added to the inside of their training boots. The students moved individually over a distance of 1,000 meters, as part of the same tactical scenario. Finally, the data was centralized according to the results received.

It was observed that the pressure applied to the insole increases on average after about 500 meters of movement (see Figure No. 5).

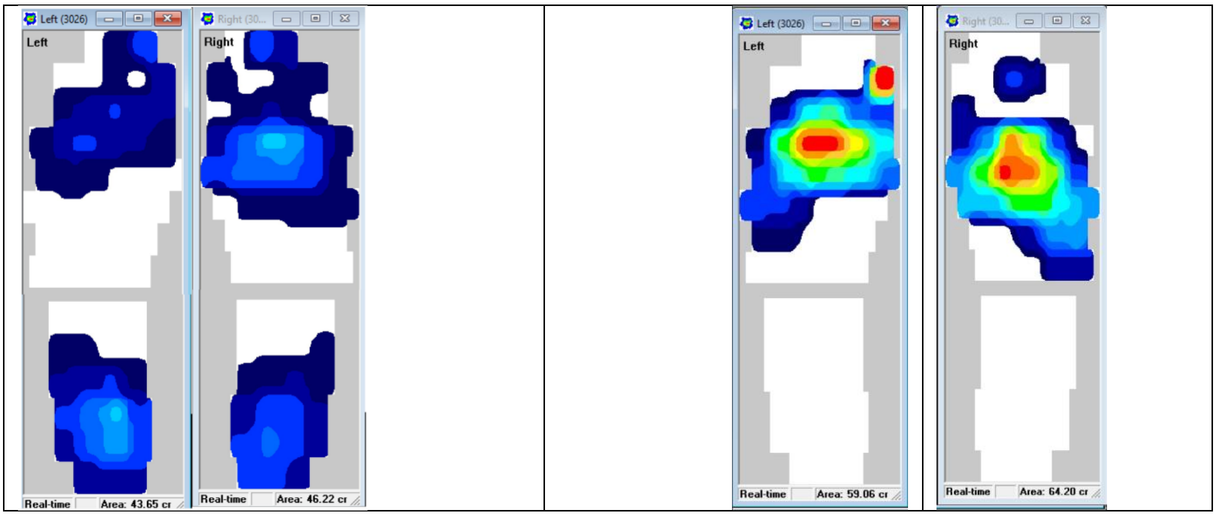


Figure no. 5. Pressure applied on the insole over a distance of less than 500 m, and more than 500 m respectively
(Source: Authors)

A graph of the pressure exerted over a period of time was created for each student (see Figure No. 6).

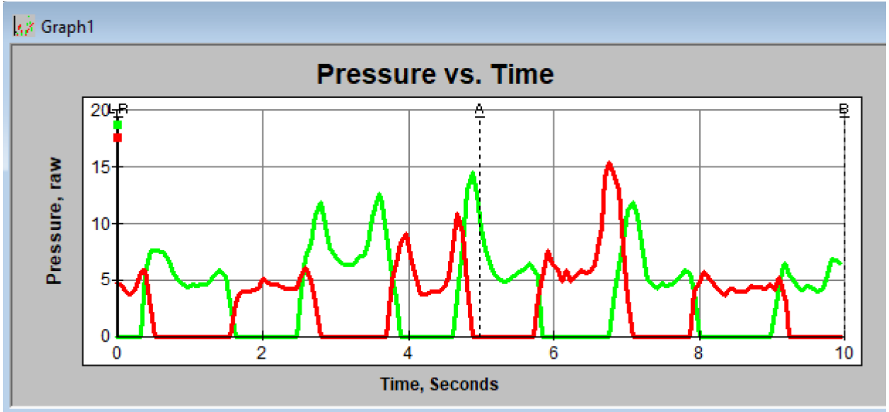


Figure no. 6. Pressure recordings over time
(Source: Authors)

A graph was also generated, containing the cadence and frequency of the steps. It was observed that the frequency of the steps decreases over time due to fatigue, respectively due to the effort capacity of each individual (see Figure no. 7).

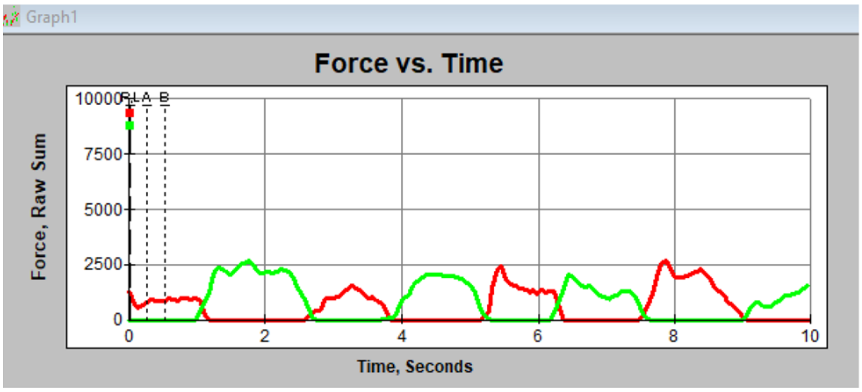


Figure no. 7. Frequency recordings over time
(Source: Authors)

The use of the MILES system (see Figure No. 8) in the analysis allowed for a realistic and efficient movement, according to the standardized procedures at the tactical level. Moreover, the continuous monitoring of military students throughout the exercises was essential for the prompt identification and correction of errors, thus ensuring optimal training and constant improvement of their operational skills.

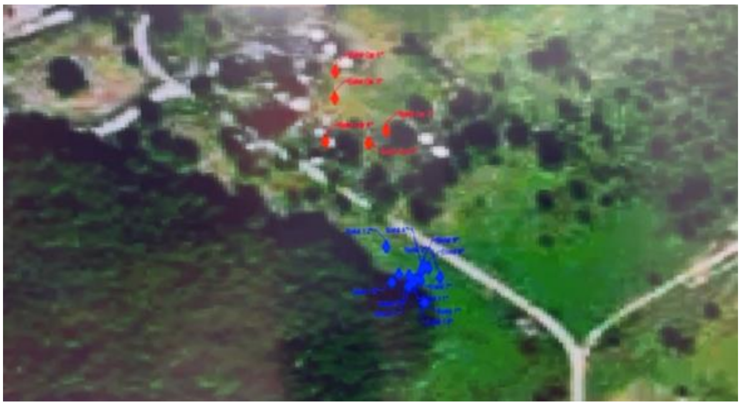


Figure no. 8. MILES instrumentation/monitoring
(Source: Authors)

Based on the collected data, we obtained the average pressure on the foot, in military footwear, for each subject. This provided an overview of the level of pressure felt by the soldiers' feet along the entire route. Low-pressure variability at the beginning of the route indicated a uniform distribution of pressure, while high variability indicated the points of imbalance, i.e. the non-uniformity of the pressure applied to the sole of the foot.

The critical pressure points appeared towards the end of the route, and these most often lead to discomfort and represent the place where the pressure on the sole is the highest.

Step frequency is a key factor that determines the pressure applied to the lower limbs, and its increase is directly proportional to the increase in fatigue and the decrease in the exercise capacity of individuals.

In this research, we analysed the results collected from measurements of the pressure exerted in military footwear on the feet, in various field contexts and military missions. Through the use of modern pressure mapping technology and advanced data analysis, we have been able to highlight several aspects relevant to understanding the impact of these factors on military performance and health.

One of the main conclusions of the study is that the distribution of pressure exerted on the foot in military footwear is essential for the comfort, performance, and safety of soldiers during missions. We found that evenly distributed pressure can indicate the comfort of military footwear and can positively influence performance in field activities. At the same time, we have also identified the critical pressure points, which appear towards the end of the route, and which can lead to discomfort and an increase in the risk of accidents or injuries. This aspect is particularly important in the military context, where a single second of delay or loss of efficiency can have serious consequences.

In addition, we observed that step frequency is a key factor in determining the pressure applied to the lower limbs, and its increase is directly proportional to the fatigue and decreased exercise capacity of the military. Therefore, it is essential to consider this particular aspect in the development and testing of different types of military footwear.

Thus, by developing these new syntheses, we have managed to make a significant contribution to the detailed understanding of the impact of military footwear on the performance and health of soldiers in various operational contexts. These findings allow us to formulate recommendations and propose innovative solutions to improve the comfort, performance, and safety of soldiers during missions.

Conclusions and future perspectives

Measuring the pressure applied to soldiers' boots can provide important information about the comfort, performance, and health of their feet during missions or training. Evenly distributed pressure can indicate the comfort of military footwear and influence over time performance in field activities.

Using pressure sensors facilitates the collection of data on how the body weight is distributed according to the load that each subject has and therefore we can decide where the risk of fatigue or accidents occurs, thus being able to find alternatives that increase both the capacity effort and military safety.

Evaluating the effectiveness of different types of military footwear is much easier to do by applying pressure sensors during different types of missions.

According to the study, the stiffness of military boots can negatively influence walking speed and walking stability, especially on uneven surfaces such as the battlefield. Therefore, increased stiffness of footwear may increase the risk of injury or decrease performance during military operations. Data collected from the analysis regarding the pressure exerted on the lower limbs, in this case on the sole of the foot in military footwear during movement, can locate critical pressure points that can lead to discomfort and an increase in the risk of accidents or injuries. Thus, a rigorous analysis of the frequency of military actions developed by planners/instructors based on these critical pressure points is recommended. Incorrect pressure distribution can be a risk factor for military personnel. Increasing the frequency of steps during movement can be associated with excessive fatigue. Fatigue can lead to a decrease in exercise capacity and an increase in the risk of injury during military operations.

Detailed analysis of the impact of lower limb pressure in military footwear on military performance and health in the tactical field/battlefield is critical to the effectiveness of military operations. The integration of the MILES and F-Scan 64 systems into military boots allows precise monitoring of the distribution of pressure on the sole of the foot and the individual/collective movement of the military. This integration enables the identification of critical pressure points and helps adjust training and equipment to minimize injury risks and maximize battlefield performance. Constantly evaluating data and continuously using these systems during training ensures that the military is prepared for modern challenges and able to respond effectively, under realistic conditions in any combat scenario.

Future research directions propose the testing of different types of footwear, and data collection and analysis of the safest, most pragmatic, and comfortable boots for the different types of missions in theatres of operations by using pressure sensors.

In the future perspective of our research, we aim to expand and diversify our approach by experimenting with research methods and techniques in varied sociocultural contexts. To gain a deeper and more comprehensive understanding of the phenomenon, it is essential to also consider the sociocultural factors that influence how soldiers perceive and adapt to military footwear and field conditions. Therefore, in the future, our research will pursue collaboration with interdisciplinary teams and apply research methods and techniques specific to the sociocultural contexts in which the military is engaged. These could include ethnographic studies, qualitative interviews, or participant observation in military units or communities with strong military traditions.

BIBLIOGRAPHY:

1. Böhm, H., & Hösl, M. (2010). Effect of boot shaft stiffness on stability joint energy and muscular co-contraction during walking on uneven surface. *Journal of Biomechanics, 43*(13), 2467-2472. https://doi.org/10.1016/j.jbiomech.2010.05.029 (In-text citation: Böhm H., Hösl M., 2010, 2467-2472)
2. Budescu, E., 2013. Biomecanică Generală, Iaşi, Tehnopress (In-text citation: Budescu, E. 2013, 3)
3. Cikajlo I, Matjacić Z. 2007 “The influence of boot stiffness on gait kinematics and kinetics during stance phase”. Ergonomics. DOI: 10.1080/00140130701582104 (In-text citation: Cikajlo I, Matjacić Z, 2007)
4. Federation of American Scientists, 1999 “Multiple Integrated Laser Engagement System (MILES)”.https://fas.org/man/dod101/sys/land/miles.htm (In-text citation: Federation of American Scientists, 1999)
5. J. D. Simpson, H. DeBusk, C. Hill, A. Knight, H. Chander, 2018. „The role of military footwear and workload on ground reaction forces during a simulated lateral ankle sprain mechanism” The Foot, Volume 34, Pages 53-57, https://doi.org/10.1016/ j.foot.2017.11.010 (In-text citation: J. D. Simpson, H. DeBusk, C. Hill, A. Knight, H. Chander, 2018, 53-57)
6. Tekscan. n.d. Last accessed February 5, 2024. https://www.tekscan.com/applications/ foot-pressure-measurement

1053477-3045-1396-24-15

CONCEPTS REGARDING THE USE OF NAVAL DRONES FOR THE ESTABLISHMENT OF A MARITIME EXCLUSION ZONE AT THE BLACK SEA

Marius MĂNĂILĂ
master's degree student, the Naval Forces Department, the Command and Staff Faculty,
„Carol I" National Defense University, Bucharest, Romania
E-mail: manaila.f.marius@gmail.com

Alin DOGARU
master degree student, the Naval Forces Department, the Command and Staff Faculty,
"Carol I" National Defence University, Bucharest, Romania
E-mail: ing_dogy@yahoo.com

***Abstract**: In this article we want to make a detailed analysis focusing on the strategic potential of naval drones in establishing a maritime prohibition zone in the Black Sea, offering a comprehensive perspective on the impact of this technology in a complex geopolitical context. By highlighting the advantages, challenges and geopolitical implications, this study aims to reveal how the use of naval drones can influence regional security and the management of sea lanes. During the paper we will analyze the advantages brought by naval drones, emphasizing the possibility of effective surveillance of maritime areas and their ability to provide a rapid response to potential threats. Comparing these capabilities with traditional maritime surveillance methods highlights the efficiency and flexibility that naval drones can bring to the creation and maintenance of a maritime no-go zone in the Black Sea.*

The research methods we proposed to use are predictive, as this observation and attack platform is still at the beginning of the road and we do not have concrete data in this regard, as well as the comparison, to be able to emphasize the advantages of this new technology .

The analysis expands on the case study, providing concrete examples of the use of naval drones in various strategic scenarios in the Black Sea. It shows how this technology can contribute to preventing illegal activities and countering threats to national security, thus strengthening Romania's strategic position in the region.

In addition, the geopolitical and diplomatic implications are examined, anticipating the reactions of riparian states and assessing the diplomacy required to successfully implement a maritime no-go zone. By bringing into discussion the specific challenges of the Black Sea, such as geo-climatic factors and cyber security, this study aims to provide a balanced approach to the implementation of this technology in a complex strategic environment.

***Keywords**: Black Sea, maritime exclusion zone, naval drones, naval forces, surveillance, strategy, technology, potential, threats.*

Introduction

In this article, we aim to conduct an analysis focusing on the strategic potential of naval drones, as well as to identify certain concepts regarding the establishment of a maritime exclusion zone in the Black Sea, providing a comprehensive perspective on the impact of this technology in a complex geopolitical context. By highlighting the advantages, challenges, and geopolitical implications, this study aims to reveal how the use of naval drones can influence regional security and the management of maritime routes.

Throughout the work, we will analyze the advantages brought by naval drones, emphasizing their ability to efficiently surveil maritime areas and their capacity to provide a rapid response to potential threats. By comparing these capabilities with traditional methods of maritime surveillance, the efficiency and flexibility that naval drones can bring to the establishment and maintenance of a maritime exclusion zone in the Black Sea are highlighted.

The Black Sea basin and its coastal countries represent a strategically vital area both geopolitically and economically. In recent decades, this region has witnessed substantial changes in maritime security dynamics, given the increasing geopolitical instability in neighboring areas. In the context of these challenges, the necessity of creating a maritime exclusion zone becomes evident, and the use of naval drones represents a key tool in addressing this imperative need.

Despite being a semi-enclosed sea, which does not classify it as a globally vital area but rather a regional one, the Black Sea serves as an important maritime transit route for global trade and energy transportation. The region is also subject to significant geopolitical pressures, considering the interference of states with divergent interests and tensions regarding control over strategic maritime routes. This complex dynamic necessitates the strengthening of security in the area to protect the economic and political interests of coastal states and the international community[2].

The central motivation for implementing a maritime exclusion zone in the Black Sea lies in the need to limit access to unauthorized vessels and prevent illegal activities. This includes combating arms trafficking, drugs, smuggling, and, crucially, preventing major events such as attacks on commercial or military vessels, which can jeopardize regional stability and the safety of the population.

Naval drones represent a significant innovation in maritime security, providing an efficient and adaptable tool for the constant surveillance and monitoring of strategic areas. Equipped with advanced sensors and real-time communication capabilities, these drones can provide crucial information for making rapid decisions and implementing appropriate measures. The technological advantages of naval drones, including their mobility, increased autonomy, and ability to operate in diverse weather conditions, give them an essential role in ensuring maritime security in the Black Sea.

By combining these aspects, the implementation of naval drones in establishing a maritime exclusion zone in the Black Sea becomes a vital strategy for protecting national strategic interests and promoting stability in a region with unique and dynamic challenges.

1. Analysis of threats and specific challenges in the region

The Black Sea, with all its strategic resources, faces multiple threats, which is why establishing a maritime exclusion zone becomes essential. Threats to security in the Black Sea include piracy, smuggling, drug trafficking, and risks associated with political instability in coastal states such as Ukraine and Georgia. These complex challenges require a coordinated and proactive approach, and establishing a maritime exclusion zone represents an effective solution to counter these threats.

Control over maritime routes in the Black Sea holds vital strategic importance for regional and global stability. According to a report issued by the *International Energy Agency*[3], this region plays an essential role in energy transportation, including resources such as oil and natural gas. Therefore, the need for strict control over maritime routes becomes crucial for the safety of energy routes and the protection of the economic interests of coastal states and the international community.

Establishing a maritime exclusion zone significantly contributes to reducing the risks associated with uncontrolled naval traffic and preventing incidents that may affect national and regional security.

The fact that Russia is focusing on increasing its "soft power" and "hard power" capabilities in the Black Sea region demonstrates its crucial importance for Russia's overall strategy. The two-hybrid conflicts supported by the Russian Federation in Georgia and Ukraine, along with Russia's often-forgotten support for Transnistria, practically represent an encirclement move around the Black Sea. It is no coincidence that Russia annexed Crimea in the initial phase of its intervention during the Ukrainian revolution. Ukraine had leased long-term rights to Russia to maintain its bases on the peninsula, but full control over Crimea gives Russia greater freedom to develop its offensive and defensive capabilities, both land-based and maritime. Before annexation, the Russian fleet in the Black Sea consisted of several cruisers and destroyers dating back to the Soviet era. Intensive modernization along with fleet expansion has drastically improved the quality of Russia's naval assets in the Black Sea[4].

[2] Florin Nistor, Lucian-Valeriu Scipanov, "The Influence of the Characteristics of the Black Sea on Joint Operations," Strategic Impact Magazine, Bucharest, 2021, vol. 80, nr. 3, p. 27.

[3] https://www.iea.org/reports/ukraine-energy-profile, accessed on February 8, 2024, at 11:00 AM.

[4] https://monitorulapararii.ro/a-sosit-timpul-marilor-investitii-in-drone-navale-militare-1-33035 accessed on February 4, 2024, at 14:15.

Considering the rapid evolution of the entire spectrum of emerging elements, we have considered the most pressing threats and challenges to security in the Black Sea to be:

1.1 Threats

Political and geopolitical tensions

Political and geopolitical tensions among coastal states such as the Russian Federation, Ukraine, Turkey, and other Black Sea region states can pose threats to maritime security. Competition for control over maritime routes and energy resources may lead to conflicts or incidents.

Illegal activities and arms trafficking

The prevalence of illegal or undeclared shipments of arms and ammunition and other illegal activities such as smuggling and drug trafficking poses a constant threat in the Black Sea. These activities can affect economic and regional security.

External interference and foreign naval presence

The intervention of foreign powers in the region and the increased naval presence of non-regional countries can generate instability and affect the balance of power in the Black Sea. Adherence to maritime laws, particularly the Montreux Convention by Turkey, and by other coastal states, contributes to strengthening regional security.

1.2 Challenges

Adapting to weather conditions

The Black Sea region is subject to extreme weather conditions, including frequent storms and dense fog. These conditions pose a challenge to naval operations, requiring navigation and surveillance capabilities that are adapted to such conditions.

Cybersecurity

With the increasingly advanced technology of naval forces, the risks of cyber attacks are growing. Protecting the cyber infrastructure of naval forces and communication systems becomes a critical challenge to ensure operational security.

Maritime incident management

With intense naval traffic and the possibility of maritime incidents, managing and preventing these incidents becomes a significant challenge. This involves efficient coordination between naval forces and civilian authorities.

Addressing these threats and challenges requires an integrated strategy involving cooperation among coastal states, strengthening the technological capabilities of naval forces, investing in cybersecurity, and implementing effective protocols for managing maritime incidents. A coordinated regional approach can ensure stability and security in the Black Sea, emphasizing the importance of dialogue and collaboration among states and international organizations.

Therefore, it is evident that establishing this zone in the Black Sea is not only a reactive measure to existing threats but can also become a proactive initiative to ensure long-term stability and security in the region.

2. Naval drone technology and the advantages of usage in the Black Sea

Unmanned Surface Vessel (USV) systems, recognized as the maritime equivalent of aerial drones for military aviation, have seen substantial technological development in recent years. Although naval military drones are not yet as widespread and utilized as aerial drones, there are all the prerequisites for USVs – from small vessels to heavy autonomous ships that can have dual military/civilian purposes – to have a secure future. Unlike Unmanned Underwater Vehicles (UUVs), these drones can use classic technical instruments used for controlling aerial drones – such as communication and navigation equipment with electromagnetic waves and satellite systems, which simplifies efforts for builders in many ways[5].

Naval drones represent the pinnacle of modern technology in maritime security, equipped with a range of innovative capabilities and technological features. They are equipped with advanced sensors such as radar, thermal cameras, and sonars, allowing detailed data collection. Artificial Intelligence (AI) is often integrated for real-time data analysis and interpretation, providing a superior level of precision and efficiency in object identification and threat detection.

Compared to traditional methods, naval drones offer significant advantages. They can operate in shallow waters and confined spaces, with superior maneuverability compared to conventional vessels. Moreover, naval drones can reach difficult-to-access areas such as deltas, bays, or estuaries, extending coverage and enhancing surveillance effectiveness.

These naval platforms can cover vast water surfaces in a relatively short time frame, ensuring constant and detailed surveillance, thus significantly improving the monitoring capacity of maritime routes and suspicious activities.

In comparison to traditional naval patrol methods, the use of naval drones entails significantly reduced costs and economic efficiency, providing increased operational flexibility and rapid adaptability to the dynamic requirements of maritime security.

Thus, these advantages highlight the significant impact that naval drone technology can have on establishing and maintaining an efficient and cost-effective maritime exclusion zone in the Black Sea.

3. Types of naval drones currently operating in the Black Sea basin.

In the dynamic landscape of modern warfare, the use of kamikaze drones, as exemplified by Ukraine's strategic deployment against the Russian fleet in the Black Sea, highlights the transformative impact of asymmetric threats on naval warfare. The innovative application of these unmanned systems, such as Sea Baby, introduces a level of unpredictability that challenges traditional defense paradigms. The recent expansion of their range not only increases their operational reach but also signifies a fundamental shift in understanding military capabilities.

The compact size of USVs, remarkable speed, and potential to create chaos through distraction and stress on the ship's personnel pose significant challenges for conventional naval defense. These attributes not only make them elusive targets but also contribute to a disturbing psychological impact, diminishing the effectiveness of a ship's defense mechanisms. The unconventional nature of kamikaze drones requires a reassessment of strategies aimed at countering these agile and adaptable threats.

Equipping Sea Baby drones with missiles represents an innovative approach. Although the type of ammunition remains undisclosed, this tactic paves the way for more efficient solutions. Even if the missiles fail to hit the intended targets, their launch serves to reduce the reaction time of defending ships. This, in turn, introduces distractions and increased stress among the ship's personnel, thereby diminishing the overall effectiveness of the ship's defense mechanisms.

Looking ahead, outfitting kamikaze drones with short-range precision missiles introduces a new dimension to their effectiveness. The integration of guided missiles would enhance their accuracy and targeting capabilities.

In a world where military technologies continue to evolve, the innovative use of kamikaze drones serves as a reminder of the imperative to stay ahead in the race of technological armament. The adaptability demonstrated in these developments underscores the need for a comprehensive approach to national defense that integrates cutting-edge technologies and anticipates the challenges posed by emerging asymmetric threats in the ever-evolving landscape of modern conflicts in the Black Sea region.

We have identified below the most used, but also the most efficient surface naval drones currently used in the Black Sea conflict. These models of naval platforms can always serve as a model for the Romanian Naval Forces, which have the chance to draw lessons both operationally and financially, for the establishment of a future structure, possibly a flotilla, of such systems.

Thus, among the most important and defining technical-tactical characteristics of the Sea Baby drone, which make it one of the most prolific in terms of its own action results, are its length of 5.5

[5] https://monitorulapararii.ro/a-sosit-timpul-marilor-investitii-in-drone-navale-militare-1-33035, accessed on February 8, 2024, at 18:30.

meters, weight of approximately 1000 kg, operating range of 400 km, autonomy of 800 km and 60 hours, payload of 200 kg, maximum speed of 43 knots, navigation systems such as automatic GNSS, inertial and visual, transmission of video data of up to 3 HD video streams, and especially 256-bit crypto protection.

On the other hand, the Magura V5 drone stands out with its superior payload of 320 kg, slightly higher autonomy of 833 km, and radio communications based on transmission through aerial platforms and satellites.

4. Conceptions regarding the use of naval drones in the Black Sea

To highlight the impact and versatility of naval drones in the Black Sea, we have examined and analyzed various possible strategic scenarios to unfold in Romania's economic and military areas of interest. Thus, new technologies can be successfully applied in any of the following identified cases:

Strategic surveillance of maritime routes

Naval drones are used for continuous and detailed surveillance of strategic maritime routes in the Black Sea, such as the Bosporus Strait, and entry points into regional ports. They allow the identification and monitoring of unauthorized or suspicious vessels, contributing to ensuring the security and integrity of maritime territories.

Monitoring offshore platforms and critical infrastructure

Naval drones are involved in the continuous monitoring of offshore platforms for energy extraction and other critical infrastructure in the Black Sea. They can detect and report suspicious activities or security incidents near these sensitive areas.

Surveillance of strategic interest zones (EEZ)

Naval drones can be used to monitor zones of strategic interest, such as underwater pipelines and energy platforms in the exclusive economic zone. They can lead to early identification of potential threats to critical infrastructure and prevent sabotage or terrorist attacks.

Patrolling in vulnerable areas

In collaboration with conventional naval forces, naval drones will be involved in the constant patrolling of vulnerable areas, such as the Bosporus Strait, Snake Island, or entrances to military ports. This activity will contribute to reducing illegal activities such as arms trafficking, smuggling, and drug trafficking, as well as maintaining naval communication routes' security within acceptable limits.

Detection and monitoring of ships

Naval drones equipped with advanced recognition technology will be used to identify and monitor ships entering territorial waters without authorization.

Prohibition and Prevention

The constant presence of naval drones in strategic areas will have a deterrent effect on illegal activities. The visible and constant presence of naval drones will contribute to a significant decrease in unauthorized ship incursions and suspicious activities.

Efficient cooperation with other surveillance platforms

Integrating naval drones with other surveillance platforms, such as patrol ships, satellites, and coastal radars, will increase synergy in detecting and tracking unauthorized vessels.

Thus, identifying ways to use naval drones in the Black Sea to fulfill objectives up to the strategic level will bring significant benefits to Romania's interests, improving the surveillance and response capabilities of naval forces in the face of threats to national security.

Conclusions

The vision of recent military actions has been based on the contemporary military phenomenon, regarding the use of force through a wide range of actions, leading to a redefinition of the role of the military system. Planners have considered various actions with a pronounced inventive and anticipatory nature at the tactical level, with effects at the strategic level, actions that were based on the concept of blitzkrieg[6].

The primary impulse of the competition for regional control over the Black Sea has remained unchanged throughout centuries of conflict. Like any chokepoint in maritime space, the Black Sea allows the regional hegemon to control the commercial routes that traverse it. Two elements ensure the uniqueness of the Black Sea – one stemming from antiquity, the other from the modern era. Firstly, the geographical proximity of the Black Sea to southern Europe gives the hegemon significant influence in both regions. Control of the Black Sea requires both land and maritime power, unlike many other maritime routes where dominance only requires a fleet. Due to its proximity and its own effort, whoever holds hegemony over the Black Sea controls a significant portion of southern Europe. Secondly, Russia's dual campaign in Syria and Ukraine reveals the central role that control over the Black Sea plays in its overall strategy. The region is both a strategic objective and a resource basin. Without it, Russia could not sustain two medium-intensity conflicts simultaneously. In conclusion, control over the Black Sea facilitates Russia's effort to ensure dominance in Eastern Europe, the Caucasus, the Eastern Mediterranean, and the Middle East.

In the Black Sea, there are few capabilities to counter Russia's dominance ambitions. Turkey, the most solid regional military power besides Russia, has a relatively small number of missile-carrying frigates, supplemented by old German-built attack submarines and missile-carrying corvettes. In the absence of other external concerns, Turkish naval forces, supported by its air forces, could likely stand up to Russian forces in the region. However, Turkey's security concerns extend beyond the Black Sea region. Thus, Russia and Turkey are somewhat equal in the regional context. Romania and Bulgaria have similar naval and air forces. Currently, the Ukrainian fleet is no longer an effective combat force in the sense of its conventional use.

Thus, in accordance with the concepts presented in the last chapter, we conclude that the use of naval drones in the Black Sea brings significant benefits to Romania's interests in maritime security and national defense. By implementing them in various strategic scenarios, such as surveillance of maritime routes, monitoring offshore platforms, and patrolling vulnerable areas, these technologies contribute to strengthening the security of maritime territories and reducing illegal activities. Moreover, efficient cooperation between naval drones and other surveillance platforms, such as patrol ships and satellites, maximizes the effectiveness of detecting and tracking unauthorized vessels, consolidating the response capacity of Romanian naval forces against potential threats to national security. Therefore, the use of naval drones in the Black Sea may constitute an essential component of Romania's security strategy, consolidating its position in the region and contributing to ensuring stability and security in the country's economic and military areas of interest.

Therefore, following all the elements identified, presented, and analyzed throughout the work, as well as the experience gained during the participation in exercises conducted by the Romanian Naval Forces, we consider it opportune to create a structure that integrates and utilizes surface naval drone platforms to fulfill both Romania's strategic objectives and interests in the Black Sea, as well as the operational and tactical objectives of the Romanian army during times of peace, crisis, and conflict.

BIBLIOGRAPHY:

1. Florin Nistor, Lucian-Valeriu Scipanov, "The Influence of the Characteristics of the Black Sea on Joint Operations," Strategic Impact Magazine, Bucharest, 2021.
2. Lucian-Valeriu Scipanov, Florin Nistor, "Considerations on Military Actions Conducted in the Northern Black Sea," Bulletin of the National Defense University "Carol I", Bucharest, June 2015.
3. "Ukraine Energy Profile," International Energy Agency,Available: https://www.iea.org/reports/ukraine-energy-profile

[6] Lucian-Valeriu Scipanov, Florin Nistor, "Considerations on Military Actions Conducted in the Northern Black Sea,Bulletin of the National Defense University "Carol I", Bucharest, June 2015, p. 100.

4. "It's Time for Major Investments in Military Naval Drones," Monitorul Apărării, Available: https://monitorulapararii.ro/a-sosit-timpul-marilor-investitii-in-drone-navale-militare-1-33035
5. "Naval Drones," Ukrainian Navy, Available: https://u24.gov.ua/navaldrones.

1053477-3045-1396-24-16

USE-CASES OF ARTIFICIAL INTELLIGENCE IN MILITARY SYSTEM

Alexandra-Codruța NEAGU
Sublieutenant Engineer, Scientific Officer at Military Equipment and Technologies Research Agency, Bucharest, Romania
E-mail: aneagu@acttm.ro

Bogdan-Iulian CIUBOTARU, PhD.
Captain Engineer, Computer Science and Information Technology PhD, Scientific Researcher rank 3 at Military Equipment and Technologies Research Agency, Bucharest, Romania
E-mail: bciubotaru@acttm.ro

Abstract: *Artificial Intelligence (AI) is increasingly integrated into various sectors, including social media, online services, and complex systems like text and image generation, health condition detection, and sentiment analysis. Its role in military systems is equally significant, enhancing capabilities in areas such as combat equipment, mission planning, virtual reality simulations, and cybersecurity. This paper aims to provide a common understanding of various Artificial Intelligence applications, which have the potential to become dual-use applications: civilian and military. It discusses the advantages and disadvantages of adopting AI in current and future defense systems. AI-enabled applications in military systems may lead to superior results in planning, target identification, and image recognition. Consequently, the existence of modern applications in the defense field would minimize errors and increase productivity. This article explores several AI use-cases in the defense sector, emphasizing scenarios where human-AI collaboration is expected to increase due to new and advanced technologies. By integrating new learning and training methods, it is expected that the capabilities of military personnel will evolve, leading to a more adaptive and responsive force.*

Keywords: *Artificial Intelligence (AI); Machine Learning; AI military use-cases; military system; modern warfare.*

I. Introduction

Artificial intelligence (AI) appeared as an idea in the middle of 20s century. At that time, it was impossible to be developed taking into account the early state of computing power. It is defined as the ability of a computer system to perform complex tasks, conduct complex computations or solve various problems that require human understanding. Nowadays, this term describes a variety of technologies that are part of daily life, like Google recommendations and translations, predictions and financial forecasting, computationally intensive calculations, and health outcome intrusion detections, with continually expanding in new domains.

The field of Artificial Intelligence is broad and includes various subdomains, each offering different types of solutions. Essentially, AI encompasses the field of Machine Learning (ML), which also includes the subdomain of Deep Learning (DL). This hierarchical structure reflects the specialization and increasing complexity in the field, from the general principles of AI to specific Deep Learning (DL) learning techniques.

ML advances and can learn and analyze data, make simple predictions, sentiment analysis or facial recognition. Deep Learning deals with neural networks, using more layers than what ML manages to create, and is mainly used for text understanding, prediction, detection or extraction of information with higher accuracy, virtual assistants or image operations.

Generative AI is a method used to generate images and texts using already existing data. This type of AI is used in chatbots (ChatGPT, Copilot) or image creation systems (Midjourney); and is used for purposes from entertainment, and education to text and image generation.

In recent years, there has been a big focus on technologies using AI mechanisms, with the large amount of data gathered being used in most studies, and the technology itself managing to support the development that comes with AI.

The military system is governed by a specific hierarchy, which can be defined by individuals tasked with solving problems at micro and macro levels. Over the years, civilian and military personnel have worked closely together to develop technologies for equipping armies to keep up with the latest resources on the market.

The emergence of AI has not ceased to appear in these military systems, both on the software and hardware side. The equipment required in the armory of military personnel is diverse, depending on the role they operate, but these systems differ greatly from those of a few decades ago, all due to the inevitable advancement of technologies, which today include more elements of AI and automation that make the overall capability and work of personnel easier and better.

II. Current status

Over the years, there has been a great focus on technological development, both civilian and military. Since the adoption of Artificial Intelligence (AI), the mechanisms have increasingly been introduced into current or developing technology.

AI has developed in 3 waves, focusing on fuzzy logic and decision trees in the first wave; statistics, spam filtering or search engines in the second wave; and human-like learning methods, NLP, and Deep Learning in the third wave. [1]

Several military forces are involved in creating AI-specialized forces for integration and synchronization of the activities. This force needs well-trained specialists to develop new ideas and work directly with civil industries for further development. Education needs to be at a high level, with training on both the technical and military side for well-trained specialists. [2]

Of the existing ones, especially in the field of planning, several applications have been noted, as described in several papers [3]. These deal with decision-making – FOX-GA – which uses several genetic algorithms to create a variety of possibilities that can be considered in the decision choice; the management system – CTAPS – is an open system, originally created for the USA Air Force, the software can be reused to help the evolution of the defense department, but also modified for its own uses; crisis planning – JADE – has integrated AI mechanisms to provide sensitive information quickly; strategic planning – DART – used to create plans quickly, and receive updates as troop numbers change; crisis systems, which was created to integrate AI capabilities into planning systems; transportation and logistics problem-solving systems – TRIPS – which includes transportation planning models created using the TRAINS system.

In addition to planning systems, there is an interest in CFG systems [4], target recognition, and terrain simulation, which help to improve the training of military staff in the long term.

Other examples where these AI mechanisms can be applied, as also specified in [5], are in the surveillance domain, in radars, ships, and electronics; in the maritime domain for underwater mine war frames, but also in cybersecurity [6].

III. Artificial Intelligence in military systems

Artificial intelligence is increasingly being adopted in the military sector. Various technologies either are under development or could potentially be developed in the future. Already in use, AI-enabled applications are:

- Simulations, which help to train specifically in various scenarios;
- Mission planning;
- Movement prediction;
- Combat equipment automation;
- Prediction of logistics consumption;
- Improving physical and cyber security;
- Systems for air force automation and remote control;
- Software and hardware are autopilot systems;

- Real-time object, person and behavior detection;
- Automated drones;
- Military robots;
- Naval force detonation and safety systems, etc.

Like any technology, there are both advantages and disadvantages in using and integrating them into existing systems. The **advantages** of AI include a decrease in human error, faster speed of operations, and increased efficiency due to the handling of large volumes of data. Additionally, AI contributes to enhanced security, allows for stand-alone development, and facilitates the replacement of manual work. The **disadvantages** of AI encompass the potential for inaccurate results due to random manual interventions, a prolonged duration for developing solutions, and the rapid pace of domain evolution, which brings new challenges before current ones are resolved. There is also a need for accredited and large volumes of data. Additionally, AI can sometimes lead to breaches of ethics.

Military systems are divided into several subdomains, including operational, logistical and planning, and cognitive-emotional. Each system may belong to more than one sub-domain, being helpful in both planning and operational mode; or in operational and cognitive mode.

3.1. Automated system

The applications in this area have the most influence on the performance of application missions through the technologies used. New resources can be used to develop automated systems, for land, sea and air vehicles, and to improve weapons. For example, automatic targeting or target monitoring systems. AI mechanisms can quickly adapt and learn from past situations to give the best results now and in the future. This is used in strategy development, where a multitude of factors are considered without the risk of omission or human error.

3.2. Real simulations

AI has come to be used to a high level in modern games as well, with complex graphics for movement generators, character awareness but also various combat situations. Using similar mechanisms, training simulations for operational military training can be created, to obtain a training capability that minimizes the specific risks. CGI simulations are a technique that modifies, alters and creates 3D images that can be used in various virtual reality scenarios. These simulations create different spaces and encounter scenarios, on different difficulty levels and of different types. Military personnel can experience teamwork, stress resistance, various strategies, improved training and remote working, providing a near-realistic experience at reduced costs and risks.

3.3. Security

Another need for advanced technologies and modern resources is perimeter security, using biometric systems for rapid identification of staff. High-performance systems can use different input data, from audio, face and/or fingerprint recognition to secure password storage or multi-factor log-in. AI enhances security by recognizing personnel from images, detecting movement and routes, detecting routine changes in detention centers, and verifying access of unauthorized people in different premises based on camera data and not only. The use of systems that perform the recognition automatically increases the performance of security staff, both in carrying out routine checks and in crises.

3.4. Cybersecurity

With increasing cyber-attacks and the focus on cyber warfare, Homeland Security has mobilized its forces to defend network security and improve it. Mechanisms for detecting, preventing and recognizing attacks are now being automated using several mechanisms based on high-performance algorithms that constantly keep learning, using Machine Learning and Deep Learning. Advanced protection against phishing, spam, network, behavioral analytics and other attacks can be achieved. AI applied in these types of protections are cost-effective, replacing the need for security experts to perform manual tasks with the possibility of delegating them to intelligent algorithms and focusing on improving them. The absence of humans and replacement with artificial intelligence eliminates the risk of human error.

3.5. Mental health assistance systems

The involvement of automated technologies in the emotional domain could be considered one of the most challenging steps in developing high-performance solutions in the military. Working directly with an individual's emotions and experiences may lead to unwanted outcomes. Even so, several research studies encourage the stress detection and monitoring, with several mental disorders that may arise due to the experiences of military personnel or changes in behavior. Prevention and early detection would help with the long-term effects of trauma and emotions. Itt is a crucial step towards improving the system by creating a safe space with a focus on both physical and mental health.

3.6. Post-accident recovery

Advances in technology have improved the quality of life for people who have suffered accidents resulting in the loss of a limb. Statistically speaking, military personnel are more likely to lose a limb than a civilian with an average age of 25 years, compared to civilian personnel with an average age of 40 years [7]. A version of this technology, already available in the market, combines artificial intelligence mechanisms with motion detection to predict individual movements. It uses a range of sensors and learns from movements over time. This would aid in the quick and healthy reintegration of injured individuals back into society. Involving AI techniques would help create the mechanism of 'muscle memory' which once introduced to artificial limbs would create a more natural range and easier life for those with this type of need.

3.7. Real-time translation systems

Other systems that use AI mechanisms are speech-to-text transformations that can be used in meetings, discussions for easier organization of ideas, and faster distribution of summaries to non-participating delegations. Such software can be integrated with encryption technologies that would make transmission, storage and reading more secure and faster. Real-time translations and transcriptions would help the accuracy of the concepts developed as well as the speed of transcription.

3.8. Mission/transcript planning and decision making

On the offensive side, mission planning, helping to make objective decisions or even risk assessment in a moment of impasse are the systems that could need AI mechanisms. For good organization, mission planning, transport, logistics, services, and tasks have a very important role in the optimal functioning of a team. Organization and planning involve discipline, which may be complex, time-consuming, and fallible. Introducing automation into decision-making, automatic computation, and focusing forces on other areas can improve long-term results.

Decision-making can be simplified by creating rules, both in an algorithmic and an automated way. Simplifying these tasks would help improve leadership, workflow, and employee interaction, with only the most important issues being discussed on a routine basis and common ones being solved automatically by specialized software using intelligent algorithms.

3.9. Risk assessment for different scenarios

Because of the speed with which processes are carried out, quick decisions can make the biggest difference at the end of missions. Software that succeeds in creating a simplified decision-making environment might be the best option for prudent filtering, yet still yield the best results.

Such systems can be trained on existing scenarios, but also on synthetic scenarios created specifically for this stage of the system. Users would simplify their lives by activating a second brain for decisions, which would help considerably in the speed of reaction, correctness, and elimination of human errors.

3.10. Resource analysis and planning

A final area discussed in which AI mechanisms can be integrated is the area of planning. This includes logistics planning of resources, in an automated way, which could eliminate the time required for regular inventory, and eliminate human errors encountered when allocating supplies.

Other systems that could be improved are duty, shift and shift planning, with systems able to consider time off, holidays or planned missions. Such systems save time, eliminate errors and create accurate and random planning.

V. Conclusions

AI can improve almost any system, but its rapid development may create an undesirable acceleration that cannot be controlled, according to several experts in the industry. In the military, these technologies could create more prepared military personnel without destroying the integrity of missions or training; help in the medical field, before, during, and after military interventions; and create an ease of understanding more concepts. Integrating AI mechanisms into existing systems, or creating new systems using AI can improve the organization and handling of data much more efficiently and quickly.

Systems such as advanced physical and network security create a more secure space effective against human error, with everything being automated. Collecting data in computational memory creates the need for less physical space, which is safer from accidents. It has been shown how the advancement of technology has helped society, and especially the military in its development.

Before long, the use of AI in routine military operations will become common. This will shift the focus of military personnel towards process optimization, rather than engaging in repetitive and monotonous tasks. From automated targeting systems, GPS, secure access, object detection, medical robots, terabyte-sized databases, the military must adapt and adopt.

In conclusion, by integrating artificial intelligence into modern technologies, the results can be considerably improved by the new techniques. The existence of AI applications in each individual's lifestyle has already proven its advantages by improving daily activities and making the technology available for end-users. Including new AI-based technologies in the military system can increase the potential of personnel and missions, advancing in tandem with global evolution.

BIBLIOGRAPHY:

1. I. Szabadföldi, "Artificial Intelligence in Military Application – Opportunities and Challenges," *Land Forces Academy Review*, vol. 26, no. 2, pp. 157–165, Jun. 2021, doi: 10.2478/raft-2021-0022.
2. N. D. Bastian, "Building the Army's Artificial Intelligence Workforce," *The Cyber Defense Review*, vol. 5, no. 2, pp. 59–64, 2020, [Online]. Available: https://www.jstor.org/ stable/26923522
3. A. Bedrouni *et al.*, "A.Guitouni. A survey of military planning systems A Survey of Military Planning Systems," 2011. [Online]. Available: https://www.researchgate.net/publication/ 228437196
4. L. Campbell, A. Lotmin, M. M. G. DeRico, and C. Ray, "The use of artificial intelligence in military simulations," in *1997 IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation*, IEEE, pp. 2607–2612. doi: 10.1109/ICSMC.1997.635328.
5. P. Svenmarck, L. J. Luotsinen, M. Nilsson, and J. Schubert, "Possibilities and Challenges for Artificial Intelligence in Military Applications," 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:161054489
6. I. Szabadföldi, "Artificial Intelligence in Military Application – Opportunities and Challenges," *Land Forces Academy Review*, vol. 26, no. 2, pp. 157–165, Jun. 2021, doi: 10.2478/raft-2021-0022.
7. R. M. T. Staruch *et al.*, "Comparing the surgical timelines of military and civilians traumatic lower limb amputations," *Annals of Medicine & Surgery*, vol. 6, pp. 81–86, Mar. 2016, doi: 10.1016/j.amsu.2016.02.008.

1053477-3045-1396-24-17

MODELLING AND SIMULATION AS A SERVICE (MSaaS) PLATFORMS – THE ROAD TO NATO MSaaS PORTAL

Elena-Lavinia IAGĂRU, PhD. candidate
Lieutenant, PhD. candidate, Military Science, National Defense University "Carol I",
Bucharest, Romania
E-mail: iagaruelenalavinia@yahoo.com

***Abstract**: In recent years, Modelling and Simulation as a Service(MsaaS) has represented one of the research directions towards which NATO has focused its efforts, thus the research groups established at the level of the NATO Modelling and Simulation Group (NMSG), had as their main objective the development and implementation of the concept within the Alliance. An MSaaS Platform represents the concrete applicability of the concept, therefore, in the specialized literature, we can identify a series of MSaaS Platforms, some based on the reference architecture proposed by NATO, and others adopting only some of its specific elements. The study of the existing MSaaS Platforms allows the identification of the current state of MSaaS implementation in the military field, providing an overview of the desirable finality of the research efforts - NATO's MSaaS Portal. The implementation of an MSaaS Portal in NATO will bring considerable benefits in the sphere of modelling and simulation, ensuring flexibility, timeliness and efficiency at low costs.*

***Keywords:** modelling, simulation, service, platform, portal, interoperability, reuse*

Introduction

Modelling and simulation represent one of the key capabilities of the military environment, being used in multiple activities in the field of education, individual and collective training, decision support, design of new equipment, procurement and many others. The field of modelling and simulation has evolved and transformed simultaneously with the changes in the operational environment, in doctrines and with the technological advance, reaching from the sandbox to systems based on virtual reality, totally immersive, in which artificial intelligence plays a central role.

The complexity of the operational environment and the speed with which it changes led to the need for a new approach in modelling and simulation, thus the concept of Modelling and Simulation as a Service (MSaaS) appeared. Previous modelling and simulation systems were characterized by rigidity, requiring dedicated workstations, predefined software specifications, and specialized personnel for operation, and could only be used in specially designed places and by a small number of people. MSaaS comes as a solution to address these shortcomings by providing flexible and reusable simulation systems, that can be used on multiple types of devices, by a large number of users, who only require brief instruction to operate the system, while reducing costs and time required to develop modelling and simulation applications.

The concept of Modelling and Simulation as a Service (MSaaS) emerged within NATO and was developed by research groups established through the NATO Modelling and Simulation Group (NMSG), the research activity of these groups is governed by a strategy of implementation of the concept within NATO that started in 2013, to be completed in 2029, when it is expected that MSaaS will reach a level of usable capability.

MSaaS is based on Service Oriented Architecture (SOA) and cloud computing and involves providing a capability that allows the development of complex simulations from simple simulation components, called services. The final desired result is represented by the implementation of an online modelling and simulation ecosystem that includes: “models, simulations, scenarios, data, tools and application services” (Patel 2019, 1-4). Within this ecosystem the user will have the opportunity to identify and select the simulation resources that meet his requirements, focusing on the reuse of existing resources, at the expense of creating new ones, he will be able to develop a complex simulation by composing these resources, simulation which can be later executed in the cloud.

Access to the MSaaS ecosystem by a user will be possible through the MSaaS Portal, which resembles an online modelling and simulation platform with a user-friendly interface. Thus, we can say that the finality of research in the field of MSaaS in NATO will be represented by the implementation of a functional MSaaS Portal within the Alliance.

Within NMSG's research efforts, a number of experiments have been carried out using prototype MSaaS Platforms, developed by industry partners, such as Aditerna SRP, NUADA and OCEAN, but the field has also developed outside of these research groups, where other MSaaS platforms have been developed and implemented by specialists in various fields or by certain companies. Some of these platforms were based on the specific MSaaS Reference Architecture proposed by NATO, others borrowed only a part of its features.

In the following, the article will present the requirements that a NATO MSaaS Portal must meet, taking into account the Reference Architecture proposed by NATO. Subsequently, the existing MSaaS Platforms, identified in the specialized literature, will be characterized from the point of view of the capabilities provided, and in the last part of the paper, an analysis will be carried out on how the platforms lend themselves to the requirements of an MSaaS Portal.

The main objective of the analysis is to provide an overview of the development of the MSaaS concept and the implementation stage of the MSaaS Portal.

1. NATO MSaaS Portal Capabilities

The Reference Architecture of MSaaS was developed by the NATO working group MSG-136 and published in the report TR-MSG-136-Part-IV *Modeling and Simulation as a Service Volume 1: MSaaS Technical Reference Architecture*, with the aim “to provide technical guidelines, recommended standards, architecture building blocks and architecture patterns that should be considered in realizing MSaaS capabilities.” (TR-MSG-136-Part-IV 2019, ES-1)

To understand the place that the Reference Architecture occupies within the entire MSaaS ecosystem, it is necessary to look at the overview of the Allied Framework of MSaaS presented in Figure No. 1. Through the Allied Framework for MSaaS, the stakeholders are connected, thus, the services developed by the providers reach the end user.

As can be seen in the figure, the central place is occupied by the MSaaS Portal, which represents the gateway through which the user interacts with the entire ecosystem. The MSaaS Portal relies on the specific MSaaS Reference Architecture and its specific Process and Governance Policies. “The users are able to discover, compose and execute M&S services through a Front-end (MSaaS Portal), which is the central access point that guides them through the process.” (TR-MSG-136-Part-III 2019, 2-2) Thus, a user has the ability to discover the modelling and simulation services available within a registry and to compose them to obtain a simulation that meets their needs and requirements. After the composed simulation is built, it will be deployed and executed in the cloud and can be used on-demand by multiple users.

To enable the discovery, composition, and execution of simulation services, the MSaaS Portal must provide a number of capabilities.

“Portal and Enabling Services capabilities include:

- Integrator Portal Applications (for creating compositions and deployment descriptions)

- Supplier Portal Applications (for providing M&S Resources and associated metadata)
- M&S Repository Services (for managing and exchanging M&S Resources)
- M&S Registry Services (for managing and exchanging M&S Resource Metadata)
- M&S Message Oriented Middleware (MOM) Services (for distributing simulation data) and M&S Mediation Services (for connecting external services and applications)
- Simulation Scenario Services (for managing simulation scenarios)" (Van den Berg n.d., 9-14; 9-15)

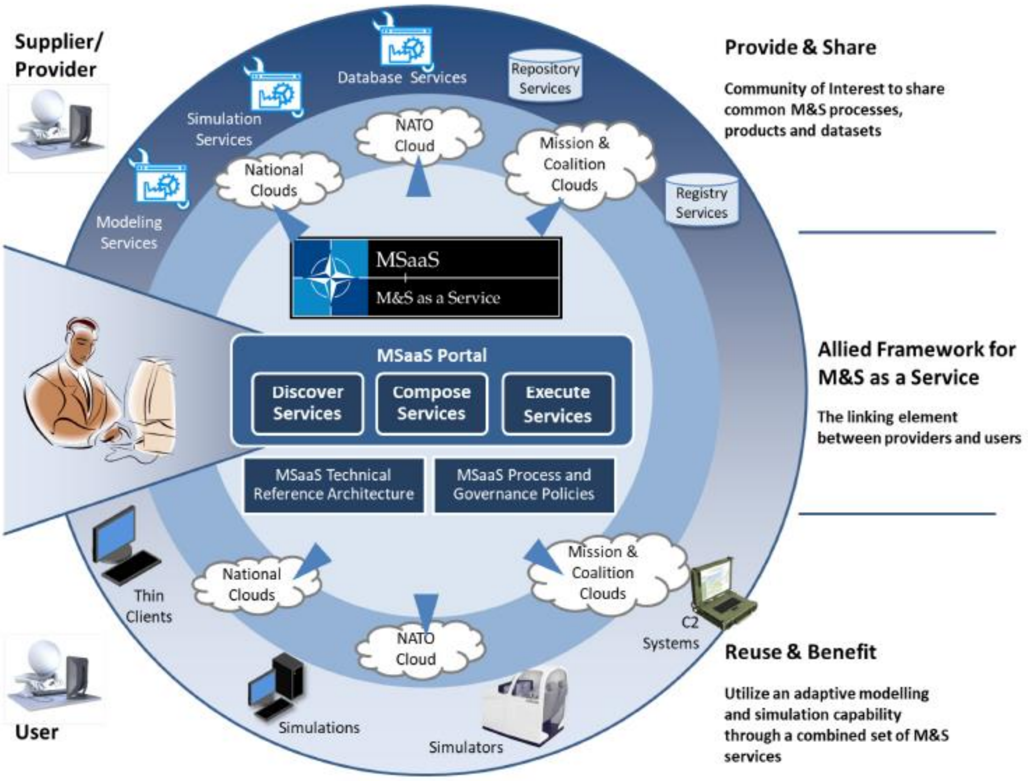

Supplier/ Provider
Database Services
Repository Services
Provide & Share
Community of Interest to share common M&S processes, products and datasets
Simulation Services
NATO Cloud
National Clouds
Mission & Coalition Clouds
Registry Services
Modeling Services
MSaaS
M&S as a Service
MSaaS Portal
Discover Services
Compose Services
Execute Services
Allied Framework for M&S as a Service
The linking element between providers and users
MSaaS Technical Reference Architecture
MSaaS Process and Governance Policies
Thin Clients
National Clouds
Mission & Coalition Clouds
NATO Cloud
C2 Systems
Reuse & Benefit
Utilize an adaptive modelling and simulation capability through a combined set of M&S services
User
Simulations
Simulators

Figure no. 1. Operational Concept of the Allied Framework for M&S as a Service (Source: TR-MSG-136-Part-III 2019, 2-2)

In addition to the capabilities of the MSaaS Portal explicitly presented, from the specialized literature we can also extract other capabilities that it must possess, such as, for example, capabilities that derive from the *Example Workflow* subsequent to *Application areas and example use cases* presented in the *Operational Concept Document (OCD) for the Allied Framework for M&S as a Service* (TR-MSG-136-Part-III 2019, 2-8; 2-12). Among them, we find the capability to choose, specify and modify scenarios and analyze data for after-action review, especially in the situation where the Portal is used for collective training.

Another feature that an MSaaS Portal must have is the existence of services that ensure information security and restrict user access within the Portal, depending on the authorizations held by each individual. Also, another important aspect that supports reuse and reduces costs is the ability to save a created simulation or parts of it, for later use within the Portal.

Because the development of the MSaaS concept derived from the need to increase the flexibility of modelling and simulation systems, so that they can be accessed on-demand, regardless of the user's location or terminal, it is indicated that the MSaaS Portal should be available for several types of devices, and to be able to achieve this, its system requirements must be as low as possible.

Given that the field of MSaaS is in its infancy, it is important that the MSaaS Portal enables the use of existing modelling and simulation resources and also ensures interoperability between services from different providers.

A central element that defines the quality of the MSaaS Portal, and implicitly of some MSaaS Platforms, is the existence of as many different modelling and simulation services as possible, as this increases the number of use cases for which the client will use the Portal.

2. MSaaS Platforms

In the specialized literature, we have identified a series of MSaaS Platforms, the characteristics and capabilities of the most relevant of them are presented below.

2.1 Aditerna SRP

Aditerna SRP is an online platform for training and data management. It offers several capabilities: "Modelling and Simulation (M&S) Resource Management, Training and Exercise Management, and M&S as a Service (MSaaS)" (Siegfried n.d., 3-3) Aditerna SRP has made available to the NMSG research groups a version of the MSaaS Portal that can be accessed through a web browser. The MSaaS Portal capabilities offered by Aditerna SRP can be found in Figure No. 2.

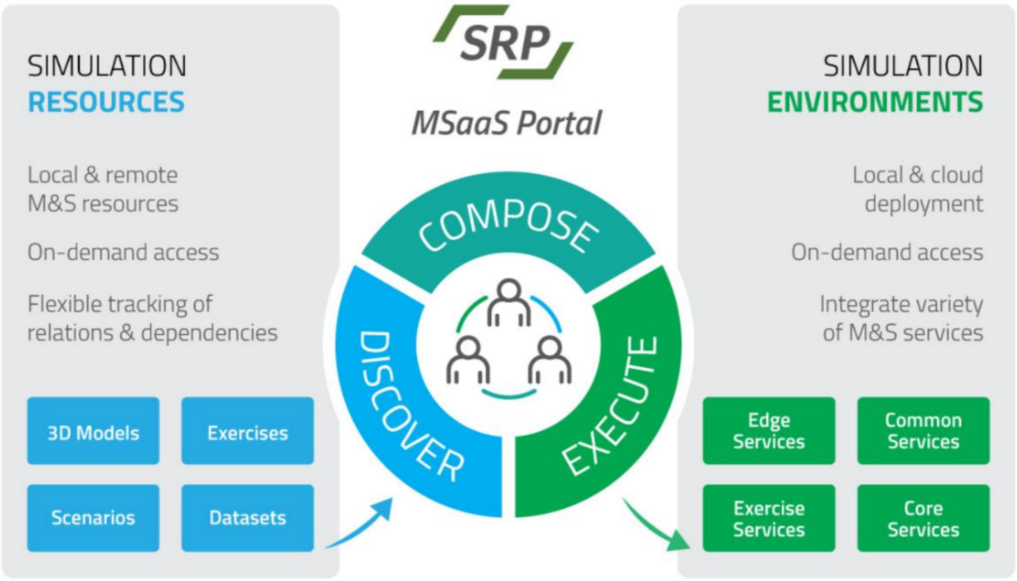


Figure no. 2. Aditerna SRP MSaaS Portal
(Source: https://www.aditerna.de/srp/)

Aditerna SRP's MSaaS portal enables the discovery, composition and execution of modelling and simulation services. As can be seen in Figure No. 2, within Aditerna SRP, the user has on-demand access to simulation resources (3D models, exercises, scenarios and datasets) and simulation environments. Simulation environments can be run both locally and in the cloud, with a considerable number of modelling and simulation services integrated within the platform.

"Aditerna SRP provides a repository for storing M&S resources, including virtual machines and containers of simulation systems, middleware technologies" (Siegfried n.d., 3-5) through it, users can access resources available in the local repository, or in partner repositories, thus allowing the use in the composed simulation of the resources made available by several organizations or providers. One of the advantages of using Aditerna SRP is represented by the fact that the deployment and execution are done automatically, without the need for user input.

The key components of Aditerna SRP for MSaaS are: The Dashboard, with the 4 predefined panels (Recently updated, Recent requirements, Recently visited, and a panel with a recommended MSaaS resource) (Siegfried n.d., 3-6), a repository for M&S services and related M&S resources and the capability to view a resource in detail, which provides information such as name, description, points of contact, pictures. screenshots, version information, documents. (Siegfried n.d., 3-8) Through these components, users can easily discover the resources that best suit their needs.

2.2 OCEAN

Leonardo is part of the MSG-136 research effort and developed, together with the NATO M&S CoE (Modelling & Simulation Center of Excellence), the OCEAN (Open Cloud Environment ApplicatioN) Platform. "OCEAN is the M&S COE solution for implementing the NATO M&S as a Service (MSaaS) approach, offering a unique point of access to services through a web portal where the users can discover, compose, and execute functions in order to facilitate the delivery, versioning, testing, consumption, termination and disposal of services."(NATO M&S CoE 2021)

OCEAN allows access to modelling and simulation applications from mobile terminals, combining resources available in the cloud with elements of virtual and immersive reality. It provides all the capabilities needed to manage a complex simulation system throughout its lifecycle.

Among the functionalities offered by the OCEAN Platform we find: (Terner, et al. n.d., 15-3, 15-4)

- Management of critical situations, outside or within military operations;
- Management of laboratories used for training or evaluation;
- Support to Concept Development and Experimentation (CD&E), in the field of doctrinal changes, equipment design and acquisitions;
- Training based on different scenarios;
- The possibility of simultaneous use of virtual and physical resources within the system;
- Reusable modelling and simulation resources available on-demand, that promote cost savings;
- A user-friendly interface that reduces the need for programming knowledge and cloud operating skills;
- Minimum required hardware elements, dedicated spaces and experienced staff;
- An Application Programming Interface that ensures interoperability with external applications.

The user interacts with the OCEAN Platform through a web Portal "which has three main functions: Discover services, Compose and Execute sessions. The web portal enables access to the services and allows managing these services according to credentials. Users can access a marketplace-type catalogue, select the services of interest and integrate them through an intuitive graphical interface in an easily reconfigurable and scalable way." (Terner, et al. n.d., 15-5) Within OCEAN, the user has access to a registry where he can discover modelling and simulation services, which he then accesses from the repository.

In the military environment, the OCEAN Platform can be used in multiple areas. OCEAN demonstrated its applicability to NATO in the Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise (CWIX) held in 2021 and 2022. OCEAN was presented as the MSaaS capability of the NATO M&S CoE and "acted in CWIX22 as Cloud Simulation Node allowing data distribution & info sharing for all the stakeholders and federating participants' M&S tools by running two specific software (PITCH RTI and C2SIM) installed on two separate Virtual Machines. OCEAN provided on cloud three different M&S tools: MASA SWORD, WISDOM (Warfare Interactive Scenario Digital Overlay Model) and COSES (Cyber Operational Synthetic Effects Service) while sharing and testing" (NATO M&S CoE 2022) partner's MSaaS capabilities in a federated environment.

Figure No. 3 shows the fields in which OCEAN can be used in military operations: cyber, naval, land, air and joint operations. OCEAN features distributed simulation elements, both live, virtual and constructive, which can be used both in individual and collective training, as well as for decision support, offering the possibility of using a considerable number of simulation environments.

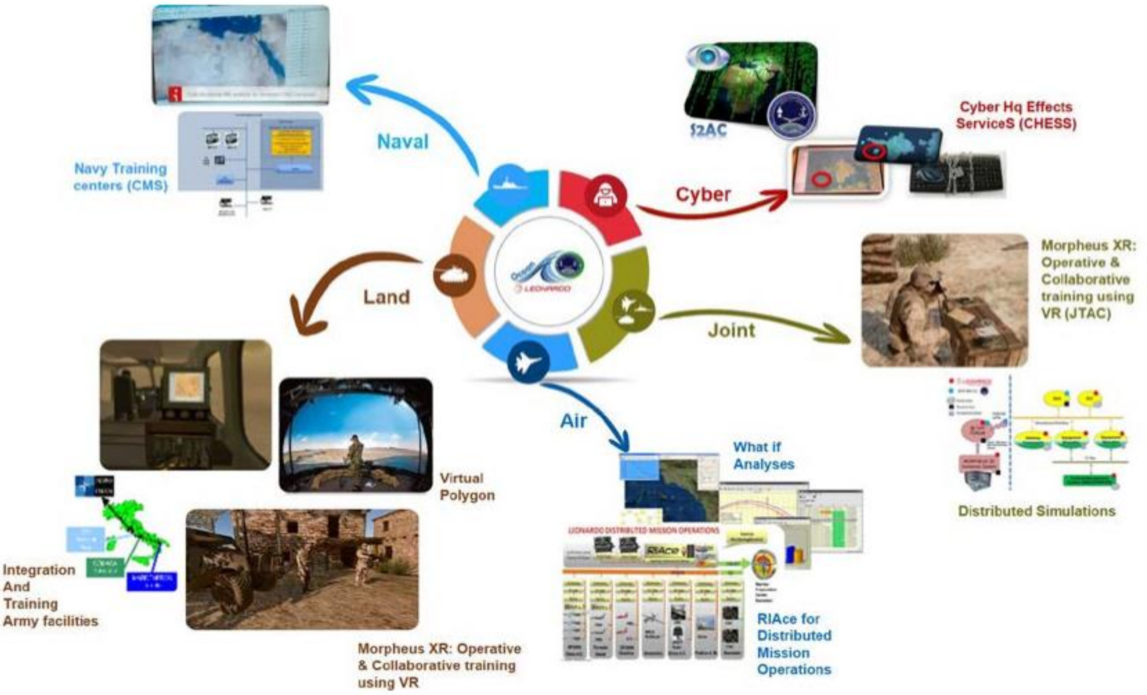

Navy Training centers (CMS)
Naval
Cyber
S2AC
Cyber Hq Effects ServiceS (CHESS)
Morpheus XR: Operative & Collaborative training using VR (JTAC)
Land
Joint
Air
Virtual Polygon
Integration And Training Army facilities
Morpheus XR: Operative & Collaborative training using VR
What if Analyses
Distributed Simulations
RIAce for Distributed Mission Operations

Figure no. 3. OCEAN Multi-Domain Application
(Source: Terner, et al. n.d., 15-6)

2.3 NUADA

NUADA is a platform developed by Thales used in activities that require a synthetic simulation environment. "NUADA reduces the amount of effort required and the time taken to set up and manage simulation-based events. It allows those who are not simulation technical specialists to easily prepare and deploy simulation environments including enabling the reuse of assets and the repetition or modification of past events. The result is a reduction in the costs of running simulation events and the ability to provide an agile response to changing requirements." (Keith n.d., 8-1)

The NUADA Platform allows the user to discover the modelling and simulation services from the repository, through a registry, the execution of the simulation environment thus being performed automatically within the platform, considerably simplifying the whole process.

A key capability offered by NUADA is that it provides a collaborative working environment where multiple users, located in different locations, can work concurrently on composed simulation development, they can easily communicate through the various communication channels provided by the platform. At the same time, NUADA allows the simultaneous participation of several users in a simulation exercise and their interaction within the simulation environment.

A simulation event can be realized within NUADA by composing the modelling and simulation services and resources available within the platform. “The NUADA user can use a drag and drop style interface to ‘compose’ an event by selecting an appropriate set of assets from those available in the system. NUADA then uses the data about the assets to intelligently define the required network, computing and software configurations such that the environment is created and set up automatically when required for use.” (Thales Group n.d.)

Within NUADA, the user is only tasked with identifying and selecting the necessary services for the simulation environment, the composition and execution being done automatically. Thus, the role of specialized technical personnel is reduced only to the stage of development of services, applications and singular resources that will be published in the registry and repository of the NUADA Platform. NUADA offers the possibility for the user to permanently monitor the state of the simulation.

Automating the composition and execution of simulation applications within the NUADA Platform is an extremely beneficial capability that reduces the time required for simulation development. However, for automation to be achieved, simulation services and resources must be perfectly compatible, which makes it impossible to use applications from sources external to the platform, decreasing the interoperability of the NUADA Platform with other MSaaS Platforms or existing MSaaS resources.

2.4 CLOUDES

CLOUDES is a Modelling and Simulation Platform developed by the Virginia Modeling, Analysis and Simulation Center (VMASC) at Old Dominion University (ODU) and is based on discrete event simulations to solve queuing problems, such as queuing at banks, supermarkets, customs, in traffic and many other situations.

“CLOUDES does so by providing a simulation environment where simulations can be designed, created, modified, executed, shared, and played with across computing platforms and operating systems by using just a web browser.” (CLOUDES User Manual v. 3.14 2014, 2) CLOUDES is intended for students and inexperienced users in order to familiarize them with the field of modelling and simulation, therefore, it has a user-friendly, drag-and-drop interface that facilitates the discovery and composition of simulation elements.

The CLOUDES Platform allows creating new simulations, modifying and using existing simulations or using predefined templates. The simulations thus created, are executed within the platform, and at the end of the execution, the user has access to the results of the simulation and the data provided by it, in order to interpret them. Due to the fact that the simulation execution takes place in the cloud, CLOUDES can be used on many types of devices without the need for high computing power, CLOUDES is available on “Firefox, Chrome, and Safari tested on desktops and iOS/Android tablets”. (CLOUDES n.d.) An example of a simulation executed in CLOUDES is presented in Figure no. 4.

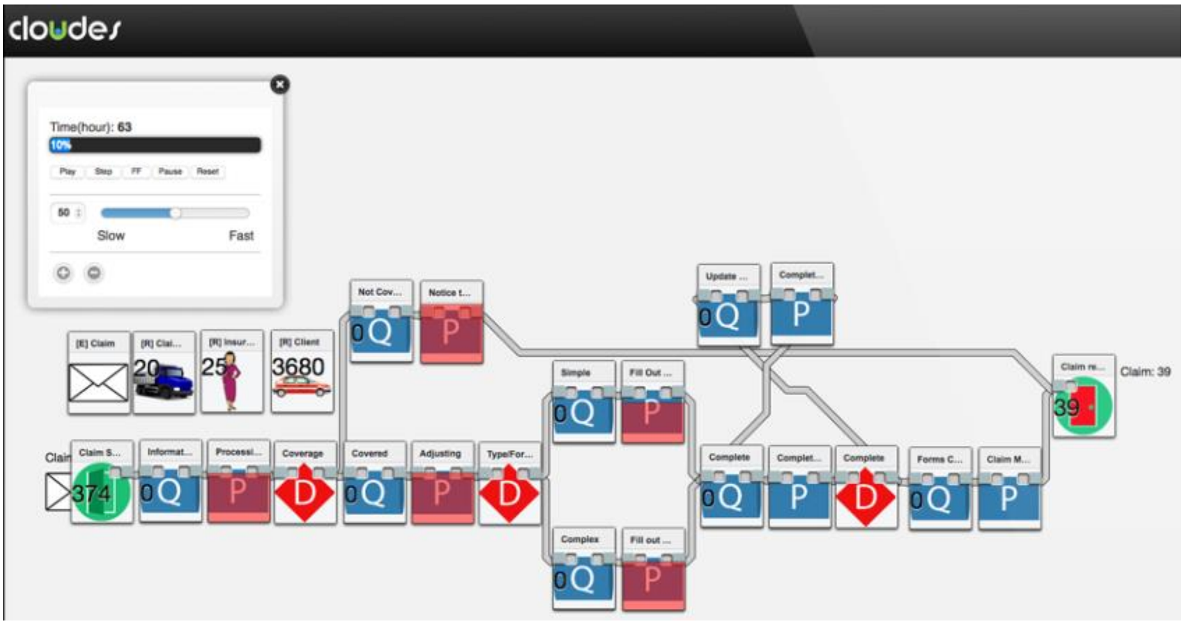


Figure no. 4. CLOUDES Simulation Example
(Source: CLOUDES n.d.)

CLOUDES represents a simplified version of an MSaaS Platform that can be useful for the initial stage of familiarizing users with the concept of MSaaS. However, the CLOUDES Platform has many limitations because the scope of use is very narrow, the type and number of modelling and simulation resources are limited, and it is not compatible with applications or resources outside the platform.

2.5 FLAMES

FLAMES (FLexible Analysis, Modeling, and Exercise System) is a simulation framework developed by Ternion Corporation for commercial and government use. FLAMES "is a family of commercial off-the-shelf (COTS) software products that provide a framework for custom constructive simulations and interfaces between live, virtual, and constructive (LVC) simulations." (FLAMES Overview n.d.)

FLAMES represents a suitable solution for the development of complex simulation applications, using the existing resources or newly developed resources. Within FLAMES, no dedicated components are simulating real-world systems; all of these components reside in registries and repositories, being developed by users or other stakeholders. The platform allows for their composition and subsequent execution of complex simulation systems. FLAMES considerably reduces the software development work required to implement a simulation application, because it integrates a considerable number of simulation support services, requiring the selection and integration of only those use case-specific components. Thus, the time, costs, and knowledge required to develop simulation environments are reduced. FLAMES encourages the reuse of existing modelling and simulation resources, as well as user-created simulation applications or parts of them, by allowing modifications to be made and the easy addition of new services or requirements.

The products offered by FLAMES are divided into two basic components: FLAMES Developer and FLAMES Engine. "The FLAMES Developer includes the tools you need to develop plugins for FLAMES that can simulate almost any system in almost any scenario imaginable. The FLAMES Engine is a set of applications that allow you to create, execute, visualize, and control FLAMES scenarios. These applications dynamically load any specified set of FLAMES plugins to allow you to create any scenario supported by the plugins." (FLAMES Products n.d.)

Through its two components, FLAMES Developer and FLAMES Engine, the Platform offers services that can be used by several categories of customers. The Developer component can be used by professional staff and industry partners to create models and simulation services to be published in the registry. The Engine component represents the Portal that can be used by the end customer to develop composed simulation applications that meet the needs of the use case, and after the simulation has been created, also through the FLAMES Engine, other users can take part in that simulation exercise.

FLAMES offers a number of extra options that aim to increase the range of capabilities offered by the platform, namely: access to Unreal Engine for the development of 3D serious games and constructive simulations (Figure no. 5), integrated services that enable complex analyses, using the Distributed Interactive Simulation (DIS) protocol to facilitate interaction between different simulations, allows communication with other simulations via High Level Architecture (HLA) based tools, multiple users can work concurrently on developing the simulation application, which can be started at any point in time in the scenario. (FLAMES Options n.d.)

Figure no. 5. 3D Simulation with FLAMES and Unreal Engine
(Source: https://store.flamesframework.com/Product/Detail?group=UCPC)

For the military domain, FLAMES offers a number of areas of use, in training, systems analysis, mission planning and mission rehearsal, wargaming, testing and evaluation.

FLAMES offers a considerable number of capabilities and services that make it a Modelling and Simulation Platform usable in multiple fields. However, the large number of modelling and simulation features increases the amount of system requirements, which restricts the type of device on which the platform can be used.

2.5 Other MSaaS Platforms

By studying the specialized literature, we also come across other MSaaS Platforms, among which we mention: Kubernetes and MSaaS in Box (Van den Berg, MSG-168: 13 n.d.), AIMS (Ford, Lloyd and Smith n.d.), hTEC (Kasım, et al. 2021), SOASim (Bocciarelli, et al. 2017), MARS (Hüning, et al. 2016). These platforms were not addressed in the paper because they are at the theoretical stage of platform design, with no usable MSaaS Platform capability.

3. MSaaS Platforms vs. MSaaS Portal Capabilities Checklist

Considering the Capabilities of a NATO MSaaS Portal described in Chapter 1 we can outline a list of features and capabilities that a Modelling and Simulation Platform must possess so that it can be considered an MSaaS Portal.

MSaaS Portal Capabilities Checklist

- Capability no.1 (C1): Discover modelling and simulation services
- Capability no. 2 (C2): Compose modelling and simulation services
- Capability no. 3 (C3): Execute composed simulation
- Capability no. 4 (C4): A registry and a repository where the user can discover the available services
- Capability no. 5 (C5): Cloud execution of simulation systems
- Capability no. 6 (C6): On-demand availability
- Capability no. 7 (C7): It allows the reuse, saving, modification and sharing of resources and applications developed by the user
- Capability no. 8 (C8): Can communicate with external simulation systems
- Capability no. 9 (C9): It is compatible and can integrate external simulation services and applications
- Capability no. 10 (C10): Management of simulation scenarios
- Capability no. 11 (C11): Provides data and information about the result of the simulation execution
- Capability no. 12 (C12): Security and restricted access
- Capability no. 13 (C13): Available on several types of devices and low system requirements
- Capability no. 14 (C14): Multi-domain applicability
- Capability no. 15 (C15): User-friendly interface

In Table No. 1, the capabilities of the platforms presented in Chapter 2 will be compared to the capabilities in the MSaaS Portal Capabilities Checklist to be able to determine if they meet the requirements to be considered MSaaS Platforms.

If the Platform possesses a certain capability, at the intersection between the column corresponding to the Platform and the line corresponding to the Capability, within the table, the symbol ✓ will be placed.

If the Platform does not possess a certain capability, the **X** symbol will be placed at the intersection between the column corresponding to the Platform and the line corresponding to the Capability, within the table.

If, after studying the characteristics of a platform, the information regarding the existence of a capability is unclear or incomplete, **ND** (no data/not determined) will be entered in the table.

Table no. 1. MSaaS Platforms vs. MSaaS Portal Capabilities Checklist

▼CAPABILITY PLATFROM►	Aditerna SRP	OCEAN	NUADA	CLOUDES	FLAMES
C1: Discover modelling and simulation services	✓	✓	✓	✓	✓
C2: Compose modelling and simulation services	✓	✓	✓	✓	✓
C3: Execute composed simulation	✓	✓	✓	✓	✓
C4: A registry and a repository where the user can discover the available services	✓	✓	✓	✓	✓
C5: Cloud execution of simulation systems	✓	✓	✓	✓	✓
C6: On-demand availability	✓	✓	✓	✓	✓
C7: It allows the reuse, saving, modification and sharing of resources and applications developed by the user	✓	✓	✓	✓	✓
C8: Can communicate with external simulation systems	**ND**	✓	**X**	**X**	✓
C9: It is compatible and can integrate external simulation services and applications	✓	✓	**X**	**X**	✓
C10: Management of simulation scenarios	✓	✓	✓	**ND**	✓
C11: Provides data and information about the result of the simulation execution	✓	✓	✓	✓	✓
C12: Security and restricted access	✓	✓	✓	**X**	**ND**
C13: Available on several types of devices and low system requirements	✓	**ND**	**ND**	✓	**X**
C14: Multi-domain applicability	✓	✓	✓	**X**	✓
C15: User-friendly interface	✓	✓	✓	✓	✓

Conclusions

Following the analysis of the characteristics of the existing MSaaS Platforms, we can conclude that in their development, emphasis was placed on the trinomial of discovery-composition-execution of modelling and simulation services, and in order to comply with this objective, registries and resource repositories were integrated within the platforms, along with support services for the automatic composition and execution of the composed simulations.

In order to increase the flexibility and accessibility of the modelling and simulation systems, platform developers have taken into account the need to ensure the availability of the platforms on-demand, correlated with the integration of a user-friendly interface to facilitate their use and increase their popularity among end-users. Most of the studied platforms have multi-domain applicability, thus increasing their range of customers.

The deficient area in meeting the requirements of an MSaaS Portal is ensuring the platform's interoperability with other simulation systems, and also compatibility with third-party modelling and simulation resources and services. Ensuring interoperability and increasing the number of automation services at various stages in the process of developing composed simulations is directly proportional to the increase in the level of system requirements, which negatively affects the number of types of devices on which the platform can be used.

Because of this, it is important to find a balance between the features offered by the platform, and the computing power required to use the simulation environment, another viable solution being the dynamic adaptation of the system requirements, depending on each individual use case.

As can be seen from the analysis, the current state of implementation of the MSaaS Portal concept is a favorable one, this being supported by the existence of platforms that have the features and capabilities foreseen for an MSaaS Portal, especially those developed in collaboration with pioneers of the MSaaS field in NATO, such as the OCEAN and Aditerna SRP Platforms. It is anticipated that NATO's future research efforts to implement the MSaaS concept within the Alliance, will focus on the integration of several existing MSaaS Platforms under the same umbrella - the NATO MSaaS Portal.

BIBLIOGRAPHY:

1. Aditerna SRP https://www.aditerna.de/srp/
2. Bocciarelli, Paolo, Andrea D'Ambrogio, Antonio Mastromattei, and Andrea Giglio. 2017. "Automated development of web-based modeling services for MSaaS platforms." *Symposium on Model-driven Approaches for Simulation Engineering.* Virginia Beach. Accessed January 26, 2024. doi: https://dl.acm.org/doi/10.5555/3108244.3108252
3. CLOUDES User Manual v. 3.14. 2014. Accessed January 29, 2024. https://beta.cloudes.me/assets/app/pdf/cloudes_manual.pdf
4. *CLOUDES.* Accessed January 21, 2024. https://beta.cloudes.me/
5. *FLAMES Options.* Accessed February 2, 2024. https://flamesframework.com/flames-options
6. *FLAMES Overview.* Accessed February 2, 2024. https://flamesframework.com/flames-overview
7. *FLAMES Products.* Accessed February 2, 2024. https://flamesframework.com/products
8. Ford, Keith, Jon Lloyd, and Neil Smith. n.d. *NATO Aligned UK Approach to Modelling and Simulation as a Service.* NATO STO. Accessed February 01, 2024. https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-MSG-149/MP-MSG-149-04.pdf
9. Hüning, Christian, Mitja Adebahr, Thomas Clemen, Jan Dalski, Ulfia Lenfers, and Lukas Grundmann. 2016. "Modeling & simulation as a service with the massive multi-agent system MARS." *Agent-Directed Simulation Symposium.* 1-8. Accessed January 27, 2024. doi: https://dl.acm.org/doi/10.5555/2972193.2972194
10. Kasım, Basar, Ahmet Birol Cavdar, Mehmet Akif Nacar, and Erdal Cayırcı. 2021. "Modeling and simulation as a service for joint military space operations simulations." *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* (SAGE Publications) 18 (1): 29-38. Accessed February 4, 2024. doi: https://doi.org/10.1177/1548512919882499
11. Keith, Ford. n.d. *MSG-168 Lecture Series on Modelling and Simulation as a Service (MSaaS)- 8.MSaaS Provider Demonstration NUADA.* NATO STO. Accessed January 13, 2024. https://www.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-MSG-168/EN-MSG-168-08.pdf
12. NATO M&S CoE. 2021. *Just finished the CWIX 2021 NATO exercise at the NATO Modelling & Simulation Centre of Excellence.* Accessed January 29, 2024. https://www.mscoe.org/just-finished-the-cwix-2021-nato-exercise-at-modelling-and-simulation-centre-of-excellence/

13. NATO M&S CoE. 2022. *Just finished the CWIX 2022 NATO exercise at the NATO Modelling & Simulation Centre of Excellence.* Accessed January 17, 2024. https://www.mscoe.org/just-finished-the-cwix-2022-nato-exercise-at-the-nato-modelling-simulation-centre-of-excellence/ .
14. Patel, Bharat. 2019. *MSG-168 Lecture Series on Modelling and Simulation as a Service (MSaaS)-1;5;7.* NATO STO. Accessed January 29, 2024. https://www.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-MSG-168/EN-MSG-168-01.pdf
15. Shahin, Mojtaba, M. Ali Babar, and Muhammad Aufeef Chauhan. 2020. "Architectural Design Space for Modeling and Simulation as a Service: A Review." *Journal of Systems and Software* 170. Accessed January 23, 2024. doi:https://doi.org/10.1016/j.jss.2020.110752.
16. Siegfried, Robert. n.d. *MSG-168 Lecture Series on Modelling and Simulation as a Service (MSaaS).* Accessed January 24, 2024. https://www.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-MSG-168/EN-MSG-168-03.pdf
17. Terner, Mathieu, Juri Barollo, Francesca Matarese, and Giovanni Tonelli. n.d. *Digitalization, Cloud, Extended Reality and Connectivity for Remote Training and Support.* NATO STO. Accessed January 18, 2024. https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SAS-165/MP-SAS-165-15.pdf
18. *Thales Group.* Accessed January 5, 2024. https://www.thalesgroup.com/en/nuada .
19. *TR-MSG-136-Part-III: Operational Concept Document (OCD) for the Allied Framework for M&S as a Service.* 2019. Accessed January 12, 2024. file:///C:/Users/LALI/Downloads/$$TR-MSG-136-Part-III-ALL.pdf
20. *TR-MSG-136-Part-IV Modelling and Simulation as a Service, Volume 1: MSaaS Technical Reference Architecture*. 2019. NATO STO. Accessed January 12, 2024. https://www.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-MSG-136-Part-IV/$$TR-MSG-136-Part-IV-ALL.pdf
21. Van den Berg, Tom. n.d. *MSG-168 Lecture Series on Modelling and Simulation as a Service (MSaaS)- 13.MSaaS Execution in the Cloud.* NATO STO. Accessed January 13, 2024. https://www.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-MSG-168/EN-MSG-168-13.pdf
22. Van den Berg, Tom. n.d. *MSG-168 Lecture Series on Modelling and Simulation as a Service (MSaaS)- 9.MSaaS Technical Reference Architecture.* NATO STO. Accessed January 10, 2024. https://www.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-MSG-168/EN-MSG-168-09.pdf

1053477-3045-1396-24-18

PERSPECTIVES AND CHALLENGES ON DRONE AUTONOMY

Cătălin BALMUȘ
Cpt.cdor. superior instructor, ”Carol I” National Defence University, Bucharest, Romania
E-mail:cata_afa@yahoo.com

Abstract: *Starting with the conflicts in Iraq and Afghanistan and extending to Nagorno-Karabakh and Ukraine, unmanned systems have played a significant role in the conduct of operations. However, they have generally been operated in a context that required remote control, with limited automation, and only for functions such as take-off and landing. In the near future, these aircraft will evolve and become increasingly autonomous, eventually transforming into true robotic systems. However, when human concepts such as intelligence, autonomy, or emotion are assigned as descriptors for machines, such as autonomous systems, intelligent robots, sensing robots, etc., confusion can arise. At the same time, it is necessary to consider the ethics of using these systems, especially when it involves technology deciding when human lives are taken.*
Keywords: *drone, autonomous, automated, autonomy levels, artificial intelligence.*

Introduction

The term „autonomous” is most probably not understood in the true sense of what it means. In the domain of defence, the term „autonomous system” is rapidly being assimilated and has quickly become a standard term. It must be understood that machines cannot be fully autonomous and only exhibit „look alike” behaviours that appear autonomous, depending on the complexity of the tasks, up to a certain level at which human control intervenes.

Increased autonomy of systems has the potential to provide a number of benefits, such as higher levels of readiness; greater speed in task execution; greater interoperability between systems; use in repetitive tasks; lower error rates; increased coordination and synchronization with other platforms; reduced risk to human life; and more. For the most part, these systems, eliminate the need for a human to be physically present in the execution of repetitive or risky tasks and often help to shorten the time for decision-making. However, these benefits come with complex legal and ethical issues and numerous technical and system design challenges.

Increasing autonomy in military systems also brings a wide range of risks, requiring changes in the planning and conduct of operations, command and control, and the training of personnel by creating new skills.

1. What is autonomy?

How can we define a system that is completely autonomous? How intelligent should „machines” be? And, ultimately, what role will humans play in this equation?

The word „autonomy” is often used randomly and in ways that do not necessarily reflect reality. When we say „autonomous robot”, for some people it means an intelligent entity that will take over the world, and for others it represents the future of human evolution. It is therefore necessary to clarify these terms and also detail known levels of autonomy.

Automation has been in practice for a long time and corresponds to a machine performing a programmed action. For example, an aircraft that maintains a certain flight level and speed, but still needs a pilot to execute the flight safely and to land. The first autopilot appeared just 9 years after the first flight of an airplane and has been used successfully since the 1920s (Voiculescu 2019).

Autonomy can be defined as the ability of a machine to perform a task without human intervention. Thus, an 'autonomous system' is a machine, whether hardware or software, that, once activated, performs a task on its own. A robot is a system (without a pilot on board) that has a degree of autonomy and the ability to perceive and react to its environment, at least in a rudimentary way (Scharre 2015).

Autonomous systems are not limited to unmanned vehicles. Many systems that have humans on board already include autonomous or automated functions. Most cars today include automated functions such as ABS (Anti-lock Braking System), traction and stability control, power steering, airbags, etc. Modern cars can include advanced driver assistance systems such as automatic lane keeping, collision avoidance, automatic parking, and even „full self-driving" capability, as Tesla claims (Tesla 2023). Military aircraft have auto-GCAS (Automatic Ground Collision Avoidance Systems) and can take control of the aircraft with the pilot on board if he becomes disoriented to avoid collision with the ground (Wright-Patterson AFB 2010). Modern commercial aircraft also have a high degree of automation available at several stages of flight. Automation has several advantages, including increased safety and reliability, improved response time and performance, reduced staff burden, especially in repetitive tasks, cost savings, and the ability to continue operations in jammed or untethered environments.

Depending on each system and its use, automated functions are intended to reduce human dependency, complement or assist human use of machines, and also assist in decision-making. These benefits raise, however, questions about the legality and ethics of the use of decision-making independence by „machines".

Although there have been many attempts to create a „level of autonomy" for a machine and to distinguish „autonomous" from „automatic" or other terms, there is currently no widely accepted definition. A definition becomes even more complicated if we try to relate it to artificial intelligence and decision-making algorithms. Therefore, true autonomy should be considered an intrinsic property of intelligent beings. Therefore, machines are not autonomous in a literal sense, but they can exhibit similar functions. If we declare that a particular function is *autonomous*, this implies a certain level of adaptation to unanticipated situations, which is different from an *automatic* function that occurs as a result of inputs, rule sets, and outputs.

Caution is needed when using the term „autonomous" in relation to machine characteristics. Rather than emphasizing that a system uses autonomous functions, it would be preferable to focus on the level of human control and responsibility and the type of automated decision-making.

We can, however, look at autonomy from three perspectives or dimensions. These dimensions can be independent, but autonomy does not exist on only one dimension but on three axes simultaneously. We can, therefore, define the dimensions or axes of autonomy as independent of the human factor, machine complexity, and the type of automated function (Scharre 2015).

Dependence on the human factor: machines that perform a function for a certain period of time, then stop and wait for human intervention before continuing, are called „semi-autonomous" or „human in the loop". Machines that can perform a function entirely on their own but have a human in a monitoring role with the ability to intervene if the machine fails to operate or malfunctions are often referred to as „human supervised" or „human on the loop". Machines that can perform a function entirely on their own and humans cannot intervene are often referred to as „fully autonomous" or „human out of the loop". In this sense, „autonomy" does not refer to the intelligence of the machine but rather to its relationship with a human controller.

Machine complexity: the word „autonomy” is also used in a completely different way when referring to system complexity. The term „automatic” is often used for very simple mechanical responses such as mechanical triggers, landmines, toasters, etc. The term „automatic” is also used to refer to more complex systems, such as self-driving cars and modern programmable thermostats. The term „autonomous” is used to define artificial intelligence, and therefore the clear boundary between „automatic”, „automated”, „autonomous”, and „intelligent” is difficult to draw.

Type of function that is automated: It is very important to specify which task or function is automated. The decisions and tasks that a machine executes have several levels of complexity and risk. Even if humans are removed from the decision-making process, a landmine or a toaster (which, once activated, use very simple mechanical switches) have very different levels of risk. As with „autonomous cars”, in the end, it is still the human who chooses the destination or tells the machine what to do. So, machines are autonomous only in certain functions.

These three dimensions of autonomy are independent, and intelligence is a different concept from the tasks being performed. Increased intelligence or more sophisticated thinking by the machine to perform a task does not necessarily translate into the transfer of control over more tasks from humans to machines. Similarly, the command-and-control relationship between man and machine is a different matter from the complexity of the tasks performed. We will still use the term "autonomy," but it will go without saying that there is some "level of automation," as I will detail later in this article.

The term "full autonomy" is not recommended to be used, and we should focus on operationally relevant autonomy, meaning sufficient autonomy to perform the tasks. Depending on the environment, the mission, the communications, and the functions required to achieve operationally relevant autonomy, they may be different depending on the scenario. In the air domain, operationally relevant autonomy could mean the ability of the aircraft to take off, land, and fly from one point to another on its own, with a human presence supervising operations and making decisions but not actually flying. In environments with heavy jamming, autonomy must be sufficient for an aircraft to continue the mission or return to base without ground control.

2. Drone autonomy levels

The types of solutions for identifying levels of autonomy vary widely, largely because there is no single authority that sets these descriptions. The best way to understand drone autonomy is to look at it as a spectrum. If autonomy is a measure of independence from external influence, then different platforms can be autonomous, but on different levels.

One of the most comprehensive approaches is that of the US Air Force Research Laboratory (Clough 2002, 5), which has defined the Autonomous Control Level (ACL): it defines 11 levels of autonomy on the four descriptors represented by the Observation-Orientation-Decision-Action (OODA) loop stages.

The US National Institute of Standards and Technology (NIST) has set up a group to address the issue of autonomy. The group proposed a framework for managing autonomy levels for unmanned systems (ALFUS—Autonomy Levels for Unmanned Systems). In the ALFUS working group, the autonomy of an unmanned system is defined as its own ability to achieve its mission objectives in relation to the three main axes: independence from human factors, mission complexity, and environmental complexity (Huang 2004, 2). As a result, more complex objectives imply higher levels of autonomy. Therefore, according to Protti and Barzan, NATO has defined four levels of autonomy (Marco Protti 2004, 7):

1. Remotely controlled system: the reactions and behaviour of the system are dependent on operator intervention.

2. Automated system: reactions and behaviour depend on fixed, built-in (pre-programmed) functionality.

3. Autonomous system without learning: behaviour depends on built-in functionality or a fixed set of rules that dictate the behaviour of the system (goal-oriented reactions and behaviour).

4. Autonomous learning system: system with the ability to modify behaviours already defined as rules for continuous improvement of goal-directed actions within a general framework of inviolable rules.

One of the most frequently used classifications of autonomy is defined by Millie Radovic in the article *Tech Talk: Unravelling 5 Levels of Drone Autonomy* (Radovic 2019).

Level 0 - No automation: the pilot is in manual control of the platform at all times.

Level 1 - Pilot-Assisted: The pilot remains in control of the overall operation and safety of the vehicle. However, the drone may take control of at least one vital function for a limited period of time. It does not have sustained control of the vehicle and never controls both speed and direction of flight at the same time, but it can provide navigation support and/or maintain altitude and position. An example would be a hobby drone (which can use GPS), but maneuvers regarding direction, altitude, and speed are done manually. These drones are typically used for inspection, maintenance, detection, photography and filming, monitoring, and security.

Level 2 - Partial automation: the pilot is still responsible for the safe operation of the vehicle and must be prepared to take control of the drone if something happens. However, under certain conditions, the drone is capable of taking control in terms of direction, altitude, and speed. The pilot is still fully responsible, including for monitoring the airspace, flight conditions, and acting in an emergency. Most manufacturers are now building drones at this level, where the platform can assist with navigation functions and allow the pilot to delegate some of his tasks. The flight path can be pre-programmed, and tasks can be executed along the way. They are mainly used for irrigation, seeding, measuring, and surveillance missions. Some drones can have automatic take-off and landing.

Level 3 - Conditional automation: the drone can fly itself, but the human pilot must still be alert and ready to take control at any time. The drone notifies the pilot if intervention is needed. This level means that the drone can perform all functions „under certain conditions”. For example, a drone that is flying on a programmed trajectory has sensors to detect obstacles and send information to the operator. He gives it the direction it needs to continue. They are mostly used for mapping and the delivery of goods.

Level 4 - High automation: the drone can be controlled by a person, but it is not always necessary to be controlled. It can fly itself in the right circumstances. It must have backup systems so that if a system fails, it is still operational. Its flight depends on a fixed set of rules that dictate the behaviour of the system. In this case, the detection and avoidance system becomes the detection and navigation system.

A private company developing drones for industry claims to have achieved this level of autonomy (Exyn technologies 2021). This appears to be the first successful demonstration of level 4 autonomy in an airborne system. Exyn Technologies has started to develop and is active in sectors such as oil and gas and infrastructure inspection. The company's drones are designed to operate in complex environments where uncertain terrain conditions can make flying dangerous.

Level 5 - Full automation: the drone controls itself in all circumstances without the need for human intervention. This includes complete automation of all flight tasks in all conditions. Such drones do not yet exist, but their future is getting closer and will pave the way for urban aerial mobility and cargo delivery. Most likely, these systems will use artificial intelligence to plan their flight, meaning they will become autonomous systems with the ability to learn and the ability to modify their already defined behaviours.

Autonomy is a feature that will increasingly be incorporated into various functions of military systems. However, the human factor will continue to be necessary, especially for tasks involving the use of force. No system will be “fully autonomous”, and even a system operating in an environment where communications will be limited will still be limited in what it is allowed to do.

3. AI vs. Autonomous

Autonomy and artificial intelligence (AI) are often used interchangeably in conversations and the media. However, these two concepts are quite different in practice. Both AI and autonomy are valuable tools and these technologies can be used independently or work together to achieve desired outcomes. In a simplified way: automation is about completing tasks and AI is about solving problems.

Robotic (autonomous) systems are designed to be used in predictable environments to complete specific, often pre-planned tasks. Sensors are very important to provide automated systems with detailed information about their place in the workspace. These systems rely on these sensors to navigate the environment and complete their tasks quickly and efficiently. Autonomous devices and systems can be guided by classical software or by artificial intelligence systems that allow them to „learn” and adapt as they operate.

Artificial intelligence is defined as a system (computer, robot, etc.) that can solve complex tasks in ways that would traditionally require human intelligence (Copeland 2023). This usually involves machine learning technologies and the use of highly advanced sensors to gather information about the environment and enable the system to react appropriately to external inputs.

Autonomous systems are already replacing humans in a wide range of tasks. In the future, these systems will be integrated throughout most sectors, and we can differentiate them, depending on the amount of human interaction required for them to work, into three main general categories:

- Direct-interaction robotic systems - are fully controlled by an operator. This process requires human intervention to perform each change in position, posture, and state.
- Operator-assisted robotic applications - require the assistance of a human operator for more complex tasks or general system management. The machine can perform certain tasks and make certain decisions, but for the most part, these systems require human intervention to choose tasks or to complete them successfully.
- Fully autonomous systems - can operate without operator assistance for long periods of time. Artificial intelligence and machine learning are often essential for these types of systems. These fully autonomous systems are preferable for use in remote areas where direct supervision is not possible or in contested environments with heavy jamming.

Control is essential for the proper functioning of robotic systems. This is why it is necessary to collect information from the environment using different sensors and combine this data through sensor fusion to process the collected data, focus on important details and information, and exercise control over the action to perform the required tasks.

Artificial intelligence and machine learning can be used at each stage to ensure that the best and most efficient solutions have been chosen for the tasks that have been assigned to the automated system.

4. Ethics and legality of autonomous systems

The use of autonomous systems for military purposes always raises questions of whether there are sufficient legal instruments that apply to these technologies and, if so, how they should be interpreted and applied in the context of technological diversity, and to what extent international laws adapt and evolve with the development of these technologies.

There are no international legal stipulations prohibiting autonomous functions in weapons systems. States are responsible for ensuring that autonomous weapons systems respect the principles of the laws of armed conflict and the principles of proportionality.

In the event of a conflict, military commanders and operators must fully understand how an autonomous system will respond to battlefield situations. They are responsible for ensuring that any future use of autonomous systems will be reasonable and that mistakes or collateral damage are minimised.

Apart from armed conflict, the use of force by autonomous systems can also occur in other situations, such as crowd control, detention, or the protection of individuals, and in such situations, human rights law is more likely to apply.

An important difference between the law of armed conflict and the law of human rights is that in the first case, it is allowed to choose targets based on the status of the target, while in the second case, it is allowed to use lethal force only based on the behaviour of the targeted person (SACT 2014, 18).

A problem may occur in assigning legal responsibility for injuries caused by autonomous systems. Although some military equipment may be able to conduct autonomous operations, this should in no way reduce a state's responsibility if it causes damage or harm. The concern is that states might try to evade responsibility for committing actions on the excuse of not knowing the flaws of the autonomous system.

There is also the ethical issue of when autonomous systems should decide on the use of force against humans. It is therefore important that developers of such systems take into account the ethical issues that may arise in their use. The ethical issues that arise from the use of unmanned aircraft could be divided into categories such as technical failures—when the system performs tasks that are inconsistent with its intended purpose; misuse—when an autonomous system is intentionally used in a way for which it was not intended; unintended consequences that arise from their use and are not anticipated from the construction phase; and, of course, the benefits gained, which often have a justification.

Despite international efforts, there is no specific, commonly accepted regulation on the use of AWS (Autonomous Weapons Systems) in armed conflict. The US Department of Defense (DoD) has issued a new directive on AWS with the potential to have a major impact on future international debate on the subject. In January 2023, the DoD issued the new AWS Directive 3000.09 (Department of Defense 2023, 3) revising the definition of AWS by replacing the word „human operator" with „operator" in the definition. We do not know yet whether removing the word „human" changes the definition to provide an option or at least opens the door for non-human operators to perform the actions outlined in the directive.

Issues of the legality and ethics of the use of autonomous armed systems were also discussed at the Retaining Meaningful Human Control of Weapons Conference, where the issue of *meaningful human control* over the initiation of an attack on a target was debated (United Nations 2018). „Meaningful human control" is a relatively new concept that can be debated from several perspectives. Firstly, *pressing a button* as meaningful human control is not sufficient, because even if the human presses the button, this does not mean that he or she has all the necessary information available, and also automation bias can occur (Kakko 2022, 8). Automation bias arises in the decision-making process because humans tend to ignore or not seek conflicting information in the case of solutions provided by the computer, especially when time is a critical factor (Cummings 2011, 1).

From another perspective, significant human control should be analysed following decisions made based on advanced artificial intelligence systems and complex, *inexplicable* algorithms (to those who use them) used by them. There is also the argument of *last resort* that has made its way into regulatory documents related to the progress of artificial intelligence. It is difficult to demonstrate what situations make *last-resort* measures correct and whether all measures are correct even in those situations.

Conclusions

Systems with simple automation have been around for a long time. As technology develops, we start to talk about complex automation or systems with some level of autonomy. There are no widely accepted regulations on levels of autonomy, but industry and authorities are working to regulate this area.

Fully autonomous systems are unlikely to emerge anytime soon, but artificial intelligence is starting to become part of these systems. For the most part, AI is used for situational awareness, data analysis, and shortening the decision-making process, but it does not involve automating all functions. It will be humans who will give the mission or create an automated system with a purpose and draw its specifications and limitations.

However, as AI becomes increasingly sophisticated, ethical and security concerns emerge about its impact on workplaces, privacy, and accountability in decision-making.

There needs to be human control at all levels of the chain of command and at the same time AI systems need to be explainable and easy to understand. The use of the *last resort* argument must be avoided in any AI regulatory text. A more comprehensive and balanced approach is needed to develop clear and strong rules in all aspects of AI.

In conclusion, we are witnessing a continuous evolution of automated systems, supported by advances in artificial intelligence. However, maintaining a level of human control, increasing transparency, and a mature debate on regulation remain essential to ensuring that technological advances are in accordance with society's values and needs.

BIBLIOGRAPHY:

1. Clough, Bruce T. 2002. *Metrics, Schmetrics! How The Heck Do You Determine A UAV's Autonomy Anyway?* Study, Wright-Patterson AFB: Air Force Research Laboratory .
2. Copeland, B. J. 2023. *Britannica.* 19 07. Accessed 07 19, 2023. https://www.britannica.com/technology/artificial-intelligence
3. Cummings, M.L. 2011. "Automation Bias in Intelligent Time Critical Decision." *American Institute of Aeronautics and Astronautics* , 1 04: 1.
4. Department of Defense. 2023. "Autonomy In Weapon Systems." *DOD DIRECTIVE 3000.09.* Deputy Secretary of Defense, 25 01.
5. 2021. *Exyn technologies.* 22 04. Accessed 06 12, 2023. https://www.exyn.com/technology/autonomous-robotics-software
6. Huang, Hui-Min. 2004. *Autonomy Levels For Unmanned Systems (ALFUS) Framework.* Interim Results, Gaithersburg, Maryland: National Institute of Standards and Technology.
7. Kakko, Yeti. 2022. *Meaningful Human Control as an Exceptional Concept.* Research internship, SaferGlobe.
8. Marco Protti, Riccardo Barzan. 2004. *UAV Autonomy – Which level is desirable? – Which level is acceptable?* Torino, Italy: Alenia Aeronautica.
9. Radovic, Millie. 2019. *DroneII.* 11 03. Accessed 06 12, 2023. https://droneii.com/project/drone-autonomy-levels
10. SACT. 2014. *Policy Guidance Autonomy in Defence Systems.* Norfolk: Supreme Allied Commander Transformation HQ.
11. Scharre, Paul. 2015. *Between a roomba and a terminator: what is autonomy?* 18 02. Accessed 12 13, 2020. https://warontherocks.com/2015/02/between-a-roomba-and-a-terminator-what-is-autonomy/

12. 2023. *Tesla.* Accessed 06 22, 2023. https://www.tesla.com/ro_ro/support/autopilot.
13. United Nations. 2018. *Retaining Meaningful Human Control of Weapons Systems.* 18 10. Accessed 08 29, 2023. https://disarmament.unoda.org/update/retaining-meaningful-human-control-of-weapons-systems/
14. Voiculescu, Alexandru. 2019. *Descoperă.ro.* 31 03. Accessed 04 03, 2023. https://www.descopera.ro/istorie/17975138-cand-a-inceput-automatizarea-avioanelor-si-cum-a-afectat-progresul-tehnologic-abilitatea-pilotilor
15. 2010. *Wright-Patterson AFB.* 4 10. Accessed 06 22, 2023. https://www.wpafb.af.mil/News/Article-Display/Article/400034/afrl-concludes-automatic-ground-collision-avoidance-flight-testing/

1053477-3045-1396-24-19

HPC COMPUTING IMPACT IN MILITARY OPERATIONS

Marius PETREA
Lieutenant Engineer, Scientific Researcher at Military Equipment and Technologies Research Agency, Bucharest, Romania
E-mail: mpetrea@acttm.ro

Gabriel Cristinel NEACȘU
Sublieutenant Engineer, Scientific officer at Military Equipment and Technologies Research Agency, Bucharest, Romania
E-mail: gneacsu@acttm.ro

Bogdan-Iulian CIUBOTARU, PhD.
Captain Engineer, Computer Science and Information Technology PhD, Scientific Researcher rank 3 at Military Equipment and Technologies Research Agency, Bucharest, Romania
E-mail: bciubotaru@acttm.ro

Abstract: *In the current military system, different activities are fundamentally based on information and information technology usage. These key elements are closely interlinked and even dependent on the current High-Performance Computing (HPC) systems. These systems may have an increased impact in military operations, both through the benefits of increasing the quantity of processed data and reducing the response time of systems necessary for carrying out activities, and by elevating the risk factor through accentuating the possibilities of creating security breaches. A prime example is the depreciation of current encryption techniques and algorithms used to safeguard and transfer information within military entities. Another factor highlighting the impact of HPC technology is the hybrid nature of its operation, utilizing central processors from computing clusters and graphical processors for the execution of associated tasks. These can serve interdisciplinary military activities in a parallel manner. This paper aims to offer an overview for the new generation of computing systems, HPCs, and to emphasize their use in military operations.*

Keywords: *High Performance Computing (HPC); Information technology; HPC military use-cases; military system; computing power.*

I. Introduction

High-Performance Computing (HPC) represents a continuously expanding technological domain that constantly pushes the boundaries of computing power and data analysis. The history of high-performance computing can be traced over the past few decades, starting with the development of the first supercomputers in the 1960s and 1970s when Seymour Cray designed the first computing machine at Control Data Corporation, achieving a performance of one million instructions per second in 1964 [5]. Initially employed mainly for scientific simulations and military applications, HPC began to extend beyond these realms in the 1980s, becoming increasingly utilized in the industry for computer-aided design. With technological advancements in the 1990s, HPC became more accessible, and solutions with distributed architectures, such as server clusters, were developed. In 1993, the TOP500 was established to classify the world's most powerful supercomputers based on the LINPACK standardized test, measuring floating-point performance [6]. A significant moment in the history of HPC occurred in the 2000s with the launch of the innovative CUDA (Compute

Unified Device Architecture) architecture by NVIDIA. This architecture introduced the ability to use GPUs for not only graphical tasks but also for general computing tasks, marking the integration of GPUs into the field of HPC. The 2010s witnessed significant progress in the miniaturization of silicon transistors, allowing for an increased number of transistors per chip, accelerating computing power and improving energy efficiency simultaneously. The latest milestone in computing power was reached in 2022 in the United States with the Frontier supercomputer at Oak Ridge National Laboratory achieving exascale performance, a level of computing known as quintillion calculations per second [2].

Projections for the High-Performance Computing field in the coming years are influenced by multiple factors, with technology rapidly advancing when it finds market demand. The COVID-19 pandemic has shifted focus to medical research, with HPC systems being utilized in molecular simulations to understand the virus and develop medication. It is anticipated that the power held by these supercomputers will be crucial in medical research, an area of continuous interest. The future is expected to bring widespread exascale computing, as multiple countries and organizations continue to be interested in developing and implementing systems capable of achieving this computing capability.

II. Current status

High-Performance Computing (HPC) technologies are key elements that provide support for a suite of domains vital to human evolution [1]:

- Medicine and Biochemistry - Through the analysis, processing, detailed modeling, and large-scale simulation using various numerical methods. Through its infrastructure and fundamental elements, HPC supports the field of Big Data Analytics (BDA). It aids in meeting the requirements of BDA activity: volume, velocity, variety, veracity, and value.
- Science and Research - The infrastructure and operation mode of HPC enable the execution of complex simulations and advanced models in related research fields. The high-processing power infrastructure supports processes such as Big Data analysis, optimization of current algorithms and techniques, design and analysis of experimental models, and, last but not least, the field of artificial intelligence. This field currently has the most significant impact, undergoing continuous expansion and evolution.
- Meteorology and Climatology - HPC supports this field by achieving much more accurate weather forecasts through precise simulations based on extensive datasets. The involvement of HPC is also evident in studying the effects of weather phenomena on natural resources.
- Financial Industry - Through the acceleration of the quantity of processed information and the reduction of processing and delivery times, HPC becomes a vital element in financial transactions. The significant impact of HPC on the industry is generated by its use as support for data mining technologies and machine learning [4].
- Automotive and Aerospace Industry - The major benefits in the automotive and aerospace industries lie in improving the design, operation, and production of molds. Another significant factor is the structural analysis of components, whether we are talking about a car or an aircraft. Each element undergoes safety and durability testing based on successive validation tests with various modeling parameters.
- Energy Industry and Natural Resources - Conducting simulations of energy processes (solar, nuclear, fossil, and hydroelectric) significantly contributes to increasing operational efficiency, optimizing, and precisely managing energy production. In addition to complex simulations performed as quickly as possible, another advantage of using HPC in the energy industry lies in designing and simulating various innovative

materials in interaction with current energy supply principles. These materials can potentially offer an alternative energy source, sometimes even with increased efficiency.

- Multimedia Industry - Computer graphics, the ability to create complex visual effects, and post-production acceleration are just a few elements highlighting the impact of multimedia data processing by a parallel computing system. The multimedia industry is a significant industrial giant that encompasses branches such as image recognition, simulation and 3D graphics, gaming, and training (through compression and encoding). All these elements generate a massive amount of raw data that requires processing and transformation into valuable information. In addition to providing very large storage capacities for the entire dataset, HPC ensures the rapid processing of this data and the delivery of information to end-users.
- Cybersecurity [3] - Within this field, the emergence of HPC technologies in the open market has led to a drastic change in the cyber ecosystem, with information storage and transfer technologies undergoing continuous evolution due to the exponential growth in processing power affecting existing security standards. Since the advent of supercomputers, they have brought about changes to both the structure and performance of the entire cyber space:
  - Rapid Data Processing – Massive impact brought about by the capabilities of swiftly processing enormous volumes of data in real-time.
  - Threat Detection – Crafting attack vectors, analyzing them, and assessing security events using advanced artificial intelligence algorithms.
  - Encryption and Communication Security – Impact brought by the continuous assessment of the robustness of encryption algorithms and their adaptation to new methods of attack. Additionally, an advantage in encryption security is provided by security simulations to test infrastructures and applications under various attack scenarios.
  - Rapid Incident Response – Impact brought about by automating incident response processes, real-time storage and visualization of incident indicators, and promptly responding to a potential attack.
  - Forensic Analysis – Leveraging HPC capabilities for the rapid and detailed investigation of recorded incidents.

In relation to the current state of domains utilizing HPC technologies, it is important to address the current trends in domains actively employing HPC systems:

- The increase in the power and complexity of HPC systems to achieve current missions' objectives.
- The growth in the processing and utilization of raw data, commonly referred to as Big Data, alongside HPC computing systems.

To increase the power and complexity of HPC systems, a current approach involves employing a hybrid architecture where supercomputers utilize both traditional processing units, known as CPUs, and graphic accelerators like GPUs or TPUs. Their activities alternate based on specific tasks. A major impact on HPC architecture will be the integration of quantum processors.

A general way to observe the importance and impact of HPC in the military domain is by dividing activities into stages:

- Data Generation Stage - Various sources generate a variety of Big Data.
- Data Processing Stage - The large volume of collected data is manipulated and analyzed.
- Data Visualization Stage - Based on the analyses conducted, information of interest for decision-making is provided.

III. HPC computing impact in military operation

At the military level, HPC (High-Performance Computing) technologies have an impact across all stages of activities, with supercomputers standing out due to three major capabilities: storage capacity, computing power (performance), and data transfer capacity (bandwidth).

- The importance of HPC in the data generation stage lies in storing large volumes of data collected from various sources (collection instruments) in real-time or at regular intervals.
- The most significant impact brought by an HPC system is in the processing stage, where large volumes of data require tools for aggregation, efficient storage, analysis, simulation, and report generation. Here, an efficient HPC system streamlines each operation through computational power, enabling rapid processing, allowing simultaneous execution of multiple algorithms, leading to the quick generation of detailed reports.
- In the data visualization stage, the HPC system ensures high speeds of transferring information of interest to commanders or decision-making systems.

The military system operates across three main categories of forces, each conducting its activities based on the three stages mentioned earlier.

In the case of ground forces, there is a variety of sources that generate Big Data with the purpose of supporting ground operations and decision-making. In the field of intelligence and surveillance, for example, various data from cameras and sensors on the ground are collected, requiring rapid processing and analysis to identify patterns and anomalies. Situations in the field can be quickly assessed, and enemy objectives and activities identified. The final information is crucial for decision-making and operational planning. In the realm of military simulations and training, processing all data related to the performance of soldiers and military equipment can easily lead to evaluating individual and team combat capabilities, identifying both strengths and weaknesses. In logistics, data regarding supply, storage, personnel, and equipment can provide commanders with vital information for decision-making in stock management, optimizing transportation routes, and reducing costs.

Within the air forces, there is the same need for real-time situational awareness. Large volumes of data from aircraft monitoring sensors, such as component status, fuel level, or weather data, as well as information about their positions, can predict potential technical issues through real-time processing. This can also determine the most efficient routes for safe arrival at a destination based on air traffic. All data from maintenance logs regarding the technical condition of an aircraft can provide information that aids in planning preventive maintenance and reducing costs.

For naval forces, data about the position of ships and maritime traffic, as well as weather, topographic and geospatial data, are useful in planning maritime routes, selecting anchorage points and can generate trajectories by anticipating critical weather conditions. Data about water depth and seafloor topography, information from sonars or radars, all of these provide real-time support for underwater operations, including submarines and diver teams, and can identify risks related to mines in maritime areas. All this sensor-derived data can accurately simulate underwater images that are crucial in planning and conducting naval military missions and exercises.

Additionally, within the military domain, research activities cover a broad range of scientific and technological applications. In medical research, analyzing the medical history of military personnel (data from medical records and health files) allows for complex analyses to create personalized medical profiles and identify individual risk factors. In the case of epidemics, analyzing epidemiological data can identify and monitor disease outbreaks in real-time, predict the spread of diseases, and simulate the effectiveness of various preventive measures for intervention planning and decision-making. In engineering, data obtained about weapon systems and ammunition used in military systems during exercises are relevant for analyzing their performance, assessing accuracy, range, and effectiveness, allowing for the simulation of their behavior in real environments and mission preparation.

IV. Conclusions

In most domains, information forms the core driving force towards the success of applications and missions. Often in a raw and complex format, of considerable size, this information requires precise analysis and an exact approach to extract their essence and character. This defining feature of information flow becomes crucial in the military domain, where speed in processing and delivering sought-after responses becomes vital. HPC supercomputers, through the use of emerging and disruptive technologies that provide processing capacity and utilization of complex data at a level of quadrillions of operations per second, have proven to be indispensable tools in accelerating the delivery of concise and precise information in the shortest possible time, with a tremendous impact on critical missions. The characteristics of HPC systems offer an interdisciplinary capacity targeting the majority of challenges that have arisen, as well as those anticipated in all fields, including the military. In conclusion, achieving strategic goals and national priorities has begun to depend on the defense system's ability to harness computing power.

BIBLIOGRAPHY:

1. K. P. A. Shajil and S. R. K. R., 2023, “ABCD Analysis of Industries Using High-Performance Computing”, International Journal of Case Studies in Business, IT, and Education, No.2 (In-text citation: Shajil 2023, 456-58)
2. Oak Ridge National Laboratory, 2022, “Frontier supercomputer debuts as world’s fastest, breaking exascale barrier”, https://www.ornl.gov/news/frontier-supercomputer-debuts-worlds-fastest-breaking-exascale-barrier (In-text citation: Oak Ridge National Laboratory 2022)
3. S. Nitin, B. Elizabeth and C. Kunj, 2022, “Cybersecurity and High-Performance Computing Ecosystem” (In-text citation: Nitin and Kunj 2022)
4. S. Yuegang and W. Ruibing, 2021, “The Impact of Financial Enterprises’ Excessive Financialization Risk Assessment for Risk Control based on Data Mining and Machine Learning” (In-text citation: Yuegang and Ruibing 2021)
5. ThoughtCo., 2019, “History of Supercomputers”, https://www.thoughtco.com/history-of-supercomputers-4121126 (In-text citation: ThoughtCo 2019)
6. TOP500, 1993, “The 500 most powerful commercially available computer systems known to us”, Last modified November 2023, https://www.top500.org/ (In-text citation: TOP500 2022)

1053477-3045-1396-24-20

ENHANCING MILITARY COMMUNICATION TECHNOLOGIES IN THE FACE OF ELECTROMAGNETIC WARFARE ENVIRONMENT THREATS

Denisa PETRAȘCU
Eng., assistant researcher, Military Equipment and Technologies Research Agency,
Bucharest, Romania
E-mail: dpetrascu@acttm.ro

Alina PLĂPĂMARU
Eng., assistant researcher, Military Equipment and Technologies Research Agency,
Bucharest, Romania
E-mail: aplapamaru@acttm.ro

Abstract: *The topic involves the intersection of military communication technologies and the challenges posed by the electromagnetic warfare environment. It explores how advancements in communication technologies must address threats arising from electronic warfare, cyber-attacks, and the complex spectrum of electromagnetic frequencies. Key considerations include ensuring secure and resilient communication channels, managing the electromagnetic spectrum effectively, and employing countermeasures to mitigate cyber-electromagnetic threats. This dynamic landscape demands a holistic approach to safeguard military communication capabilities in the face of evolving technological and strategic challenges. One of the most known solutions is related to the integration of electronic countermeasures to defend against signal jamming, interference, and other electronic warfare tactics that aim to disrupt or compromise communication systems. The modern approach is the utilization of artificial intelligence (AI) and machine learning (ML) algorithms to enhance threat detection capabilities, identifying and responding to anomalous patterns indicative of potential electronic warfare or cyber-attacks.*

Keywords: *Electromagnetic Warfare, Electromagnetic Spectrum, Cyber-Electromagnetic Environment, Spectrum Management, Electronic Warfare Operations, Communication Security.*

Introduction

In an era where the battlefield is increasingly characterized by sophisticated electronic warfare capabilities, the need for robust and resilient military communication technologies has never been paramount. The advent of electromagnetic warfare poses significant challenges to traditional communication systems, threatening the integrity, security, and effectiveness of vital military communications on the front lines. In response, military organizations worldwide are investing heavily in research, development, and implementation of advanced communication technologies tailored to operate effectively amidst the complexities of the electromagnetic spectrum (figure 1). This endeavor aims not only to maintain seamless communication between military units but also to safeguard sensitive information from interception, manipulation, and disruption by hostile forces.

Enhancing military communication technologies in the face of electromagnetic warfare threats requires a multifaceted approach that encompasses technological innovation, strategic planning, and operational adaptation. At its core, this endeavor aims to ensure the uninterrupted flow of critical information between military units while safeguarding against interception, manipulation, or disruption by hostile actors (P. H. J. Chong and N. A. Nordbotten, May 2023).

One key aspect of this effort involves the development of secure and resilient communication systems capable of operating effectively in contested electromagnetic environments. Encryption technologies play a crucial role in safeguarding sensitive data from interception, ensuring that only authorized personnel have access to classified information. Additionally, communication systems must be designed with built-in redundancy and adaptive capabilities to mitigate the effects of jamming or interference, enabling continuous communication even in the face of adversarial actions (B. M. Kannan and C. Srinivasan, 2023).

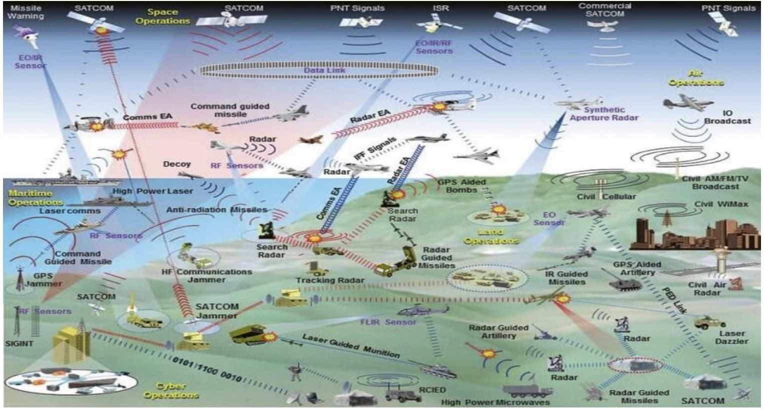


Figure no. 1. Operational domains in electromagnetic warfare scenarios
Source: https://www.nato.int/cps/en/natohq/topics_80906.htm

Advanced signal processing techniques also play a critical role in enhancing military communication capabilities. By employing algorithms for signal detection, filtering, and modulation, communication systems can effectively counteract the effects of electromagnetic interference, enabling reliable communication in noisy or hostile environments. Furthermore, the implementation of frequency-hopping and spread-spectrum techniques can help to minimize the vulnerability of communication signals to interception or jamming (R. Khodke and V. N. Dhawas, 2016)

Interoperability and compatibility across diverse communication platforms and domains (figure 2) are also essential considerations in enhancing military communication technologies. With the increasing integration of land, sea, air, space, and cyberspace operations, communication systems must be able to seamlessly exchange data and information across different domains, facilitating coordinated joint operations and maximizing situational awareness on the battlefield.

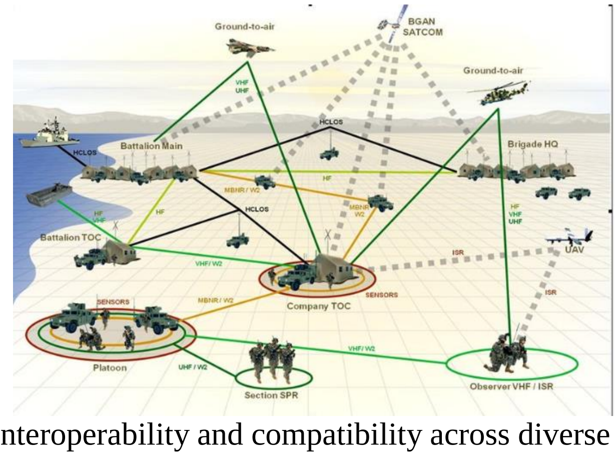


Figure no. 2. Interoperability and compatibility across diverse communication platforms and domains. Source: https://www.cyntony.com/tactical-communications-antennas

Research and development efforts are crucial for staying ahead of emerging threats and technological advancements in electromagnetic warfare. Continued investment in cutting-edge technologies, such as cognitive radio, software-defined networking, and quantum-resistant encryption, is essential for maintaining a technological edge over potential adversaries. Additionally, partnerships with industry leaders and academic institutions can provide valuable expertise and resources for accelerating innovation in military communication technologies.

In this context, enhancing military communication technologies in the face of electromagnetic warfare threats is a complex and dynamic undertaking that requires continuous innovation, strategic planning, and operational adaptation. By investing in secure, resilient, and interoperable communication systems, military organizations can ensure the integrity, effectiveness, and survivability of communication networks in an increasingly contested and adversarial environment.

To enhance the military communication technologies in the face of electromagnetic warfare threats and to provide a more resilient and adaptive communication infrastructure for military operations, different aspects such as those that will be presented next should be taken into account (L. Lazarov, 2019):

- Electromagnetic Spectrum Management:
  - Explore advancements in spectrum management techniques to efficiently allocate and utilize the electromagnetic spectrum for military communication;
  - Discuss the challenges posed by electromagnetic interference and methods to mitigate them, ensuring reliable communication in contested environments.
- Secure Communication Protocols:
  - Investigate the development of robust and secure communication protocols that can withstand electronic warfare attacks and prevent unauthorized access to sensitive military information;
  - Explore encryption technologies and quantum-resistant cryptographic methods to enhance the security of military communication channels.
- Adaptive Antenna Systems:
  - Examine the use of adaptive antenna systems to enhance the resilience of communication systems against jamming and signal interference;
  - Discuss the implementation of smart antennas that can dynamically adjust their configurations to maintain communication links in the presence of electromagnetic threats.
- Artificial Intelligence in Signal Processing:
  - Explore the role of artificial intelligence (AI) in signal processing for military communications, including real-time threat detection and adaptive modulation techniques;
  - Discuss how machine learning algorithms can analyze patterns in the electromagnetic environment to predict and counter potential threats.
- Cognitive Radio Networks for Dynamic Spectrum Access:
  - Explore the implementation of cognitive radio networks in military communication systems to enable dynamic spectrum access.
  - Discuss how cognitive radios can autonomously adapt to changing electromagnetic conditions, avoiding interference and maintaining communication links.
  - Examine the integration of machine learning algorithms to enhance the decision-making capabilities of cognitive radios, optimizing spectrum utilization in contested environments.

1 Military Communication Technologies

Military communication technologies (figure 3) play a critical role in enabling effective command, control, and coordination of military operations across diverse and dynamic operational environments. In recent years, rapid advancements in technology have led to the development of a wide range of sophisticated communication systems tailored to the unique needs and challenges of modern warfare. From secure voice and data transmission to real-time situational awareness and beyond, these technologies are at the forefront of enhancing the effectiveness and survivability of military forces on the battlefield (R. Bajracharya and H. Shin, vol. 11, 2023).

Figure no. 3. Military communication technologies
Source: https://www.semanticscholar.org/paper/IoT-Practices-in-Military-Applications-Gotarane-Raskar/e760b0e236ceec9bedc985bed3dbcd99f92805c0

One of the most significant advancements in military communication technologies in recent years has been the proliferation of secure and resilient communication systems. With the increasing prevalence of cyber threats and electronic warfare tactics, ensuring the confidentiality (R. Hermon, U. Singh and M. Khatkar, 2023), integrity, and availability of communication networks has become a top priority for military organizations worldwide. To address these challenges, military communication technologies now incorporate robust encryption algorithms, authentication mechanisms, and anti-jamming capabilities to safeguard sensitive information and prevent unauthorized access to communication channels.

Furthermore, the integration of satellite communication capabilities has revolutionized the way military forces communicate and share information on the battlefield. Satellite-based communication systems offer global coverage, high bandwidth, and low latency, enabling secure and reliable communication across vast distances and in remote or hostile environments. These systems provide military commanders with real-time access to critical information, intelligence, and situational awareness, empowering them to make informed decisions and adapt rapidly to changing operational conditions.

Tactical radios (figure 4) represent another key component of current military communication technologies, providing frontline troops with secure and resilient voice and data communication capabilities in the field. These radios are designed to withstand the rigors of combat, offering ruggedized construction, long battery life, and interoperability with existing communication systems. Additionally, advancements in software-defined radio (SDR) technology have enabled greater flexibility and versatility in tactical radio platforms, allowing for easy reconfiguration and adaptation to evolving mission requirements.

Figure no. 4. Tactical radios
Source: https://www.l3harris.com/all-capabilities/tactical-vhf-uhf-radios

In addition to these core capabilities, current military communication technologies also encompass a wide range of specialized systems and applications tailored to specific operational needs. These include unmanned aerial vehicle (UAV) communication systems, command and control (C2) networks, electronic warfare (EW) countermeasures, and network-centric warfare (NCW) architectures, among others. Together, these technologies form a comprehensive and interconnected ecosystem that enables military forces to communicate, collaborate, and coordinate effectively across all domains of warfare. Military communication technologies are continually evolving, driven by advancements in various fields, including telecommunications, cybersecurity, and artificial intelligence. Some of the current military communication technologies are:

- Satellite Communication:
  - Military forces extensively use satellite communication for long-range, secure, and global connectivity.
  - High-frequency satellite bands enable voice, data, and video transmission, supporting strategic and tactical communication.
- Secure Radio Communication:
  - Advanced secure radio systems employ frequency-hopping spread spectrum and encryption to protect against interception and jamming.
  - Software-defined radios allow for flexible and adaptive communication in various frequency bands.
- Tactical Data Links:
  - Tactical data links facilitate the exchange of real-time information between military platforms, such as aircraft, ships, and ground forces.
  - Systems like Link 16 provide secure and jam-resistant communication for situational awareness.

- Network-Centric Warfare:

  - Military communication has shifted towards network-centric warfare, where various platforms and sensors are interconnected in real-time.
  - This approach enhances collaboration, data sharing, and decision-making among different units on the battlefield.
- Cybersecurity and Electronic Warfare:
  - Military communication systems incorporate robust cybersecurity measures to protect against cyber threats and electronic warfare attacks.
  - Electronic countermeasures and anti-jamming technologies help maintain communication integrity in contested environments.
- Advanced Encryption Techniques:
  - Modern military communication relies on advanced encryption techniques to secure data transmission.
  - Quantum-resistant encryption methods are being explored to address potential future threats to classical encryption.

2 Modern threats and challenges

Military communication technologies face a myriad of threats and challenges in the context of electromagnetic warfare scenarios, where adversaries seek to disrupt, degrade, or deny communication channels vital to military operations. To mitigate these threats, military organizations must invest in robust and resilient communication systems capable of adapting to dynamic and contested electromagnetic environments while safeguarding the confidentiality, integrity, and availability of critical information. This requires a comprehensive approach that encompasses technological innovation, operational planning, and training to ensure that military forces can maintain effective communication and coordination in the most challenging of circumstances.

The threats and challenges of the current military communication technologies are (R. Bajracharya and H. Shin, vol. 11, 2023):

- Satellite Communication:
  - ***Threats:*** Satellites are vulnerable to jamming, spoofing, and physical attacks. Anti-satellite weapons pose a risk to space-based communication infrastructure.
  - ***Challenges:*** Developing resilient satellite systems that can withstand electronic warfare attacks, improving encryption for secure communication, and addressing the growing threat of space-based anti-satellite capabilities.
- Secure Radio Communication:
  - ***Threats:*** Adversaries may attempt to intercept radio signals, engage in frequency jamming, or launch cyber attacks targeting software-defined radios.
  - ***Challenges:*** Ensuring robust encryption methods against evolving cyber threats, enhancing frequency agility to counter jamming, and addressing the risk of software vulnerabilities in software-defined radio systems.
- Tactical Data Links:
  - ***Threats***: Data links are susceptible to jamming, interference, and interception. Adversaries may attempt to disrupt the flow of critical information.
  - ***Challenges:*** Developing anti-jamming techniques, improving the resilience of data link protocols, and enhancing encryption methods for secure data transmission.

- Network-Centric Warfare:

  - ***Threats:*** Network-centric systems are susceptible to cyber attacks targeting communication nodes and disrupting the interconnected network.
  - ***Challenges:*** Strengthening cybersecurity measures to protect against network intrusions, ensuring redundancy in communication pathways, and developing protocols for secure and efficient information sharing.
- Cybersecurity and Electronic Warfare:
  - ***Threats:*** Cyber threats include malware, denial-of-service attacks, and attempts to compromise encryption keys. Electronic warfare can disrupt communication through jamming and interference.
  - ***Challenges:*** Continuously adapting cybersecurity measures to counter evolving threats, integrating artificial intelligence to detect and respond to cyber attacks, and developing resilient electronic warfare countermeasures.
- Advanced Encryption Techniques:
  - ***Threats:*** Quantum computers pose a potential threat to traditional encryption methods. Adversaries may attempt to exploit vulnerabilities in encryption algorithms.
  - ***Challenges:*** Researching and implementing quantum-resistant encryption, staying ahead of advancements in quantum computing, and ensuring backward compatibility with existing systems during encryption upgrades.

Some measures and counter-measures to mitigate the threats and challenges associated with military communication technologies in the context of electromagnetic warfare scenarios are:

- Satellite Communication:
  - ***Measures:***
    - Implement frequency hopping and spread spectrum techniques to make satellite signals more resistant to jamming.
    - Deploy redundant satellite systems and establish ground-based tracking and control centers to mitigate the impact of potential attacks.
  - ***Counter-Measures:***
    - Develop anti-jamming technologies, such as nulling antennas, to protect satellite communication against intentional interference.
    - Enhance cybersecurity measures to protect ground control stations from cyber attacks.
- Secure Radio Communication:
  - ***Measures:***
    - Utilize frequency-agile radios to adapt to changing electromagnetic conditions and avoid jammed frequencies.
    - Implement strong encryption algorithms and key management protocols to secure radio communication.
  - ***Counter-Measures:***
    - Develop and deploy advanced electronic counter-countermeasure (ECCM) techniques to counteract jamming attempts.
    - Regularly update and patch software-defined radios to address potential vulnerabilities.
- Tactical Data Links:
  - ***Measures:***
    - Implement frequency diversity and error-checking protocols to enhance the robustness of data links.
    - Utilize directional antennas and encryption to secure data link transmissions.
  - ***Counter-Measures:***

        - Develop adaptive data link protocols that can switch frequencies and modulation schemes in response to interference.
        - Implement intrusion detection systems to identify and counter cyber threats targeting data links.
- Network-Centric Warfare:
    - ***Measures:***
        - Establish secure and redundant communication pathways within the network.
        - Employ intrusion detection and prevention systems to identify and respond to cyber threats.
    - ***Counter-Measures:***
        - Develop deception techniques to mislead potential attackers and protect critical network nodes.
        - Implement network segmentation to contain and isolate cyber threats.
- Cybersecurity and Electronic Warfare (figure 5):
    - ***Measures:***
        - Regularly update and patch software systems to address vulnerabilities.
        - Implement multi-factor authentication and robust access control measures.
    - ***Counter-Measures:***
        - Develop and deploy advanced anti-malware and intrusion detection systems.
        - Conduct regular cybersecurity training for military personnel to recognize and respond to cyber threats.

Figure no. 5. Electromagnetic warfare and cyber security center
Source: https://www.c4isrnet.com/electronic-warfare/2023/02/02/pentagon-tester-gives-thumbs-up-to-us-army-electronic-warfare-planner/

- Advanced Encryption Techniques:
    - ***Measures:***
        - Invest in research and development of quantum-resistant encryption algorithms.
        - Establish key management protocols that regularly update encryption keys.
    - ***Counter-Measures:***

- Monitor advancements in quantum computing and update encryption methods accordingly.
- Implement quantum key distribution for secure key exchange.

Addressing these threats and challenges is essential for maintaining effective and secure military communication in the face of electromagnetic warfare scenarios. Ongoing research and development efforts focus on staying ahead of potential adversarial capabilities and ensuring the resilience of communication systems. These measures and counter-measures are essential components of a comprehensive strategy to enhance the resilience of military communication technologies in the face of electromagnetic warfare threats. Regular updates, training, and collaboration between military, industry, and research institutions are critical for staying ahead of evolving challenges.

Conclusions

Enhancing military communication technologies is crucial for maintaining effective and secure communication on the battlefield, especially in the face of electromagnetic warfare threats. In modern warfare, the ability to communicate reliably and securely is essential for command and control, coordination of military operations, and ensuring the safety of personnel (D. Wilcoxson, 2013). Military communication technologies must be designed with adaptability and resilience in mind to withstand the challenges posed by electromagnetic warfare. This includes the ability to dynamically adjust to changing electromagnetic conditions, employ encryption and other security measures to protect sensitive information, and maintain communication links even in the presence of interference or jamming (R. Khodke and V. N. Dhawas, 2016).

Ensuring interoperability between different communication systems and platforms is essential for effective military operations. Enhanced communication technologies should be compatible with existing systems and capable of seamless integration across diverse domains of warfare, including land, sea, air, space, and cyberspace. Continued investment in research and development is necessary to stay ahead of emerging threats and technological advancements in electromagnetic warfare. This includes funding for basic research in areas such as signal processing, communication protocols, and encryption techniques, as well as the development of next-generation communication technologies tailored to the needs of the modern battlefield.

Collaboration and partnerships with industry leaders, academic institutions, and allied nations can provide valuable expertise, resources, and technological innovations for enhancing military communication capabilities. By leveraging collective knowledge and capabilities, military organizations can accelerate the development and deployment of advanced communication technologies to address the challenges of electromagnetic warfare. Effective training and education programs are essential for ensuring that military personnel are proficient in the use of enhanced communication technologies and equipped to operate effectively in electromagnetic warfare environments. This includes training on proper communication protocols, cybersecurity practices, and techniques for countering electronic warfare threats.

In conclusion, enhancing military communication technologies in the face of electromagnetic warfare environment threats requires a comprehensive and multi-faceted approach that encompasses technological innovation, strategic planning, collaboration, and training. By investing in advanced communication capabilities and adapting to the evolving nature of modern warfare, military organizations can maintain a decisive edge on the battlefield and ensure mission success in the most challenging of environments.

BIBLIOGRAPHY:

1. B. M. Kannan, P. Solainayagi, H. Azath, S. Murugan and C. Srinivasan, "Secure Communication in IoT-enabled Embedded Systems for Military Applications using Encryption", 2023 2nd International Conference on Edge Computing and Applications (ICECAA), 2023, pp. 1385-1389, doi: 10.1109/ICECAA58104.2023.10212400.
2. D. Wilcoxson, "Advantages of Mobile Broadband Communications Services for Military Applications," MILCOM 2013 - 2013 IEEE Military Communications Conference, 2013, pp. 266-272, doi: 10.1109/MILCOM.2013.53.
3. L. Lazarov, "Perspectives and Trends for the Development of Electronic Warfare Systems," 2019 International Conference on Creative Business for Smart and Sustainable Growth (CREBUS), 2019, pp. 1-3, doi: 10.1109/CREBUS.2019.8840074
4. P. H. J. Chong and N. A. Nordbotten, "Military Communications and Networks," in IEEE Communications Magazine, vol. 61, no. 5, pp. 158-158, May 2023, doi: 10.1109/MCOM.2023.10129047.
5. R. Bajracharya, R. Shrestha, S. A. Hassan, H. Jung and H. Shin, "5G and Beyond Private Military Communication: Trend, Requirements, Challenges and Enablers," in IEEE Access, vol. 11, pp. 83996-84012, 2023, doi: 10.1109/ACCESS.2023.3303211.
6. R. Hermon, U. Singh and M. Khatkar, "Cyber and Electronic Warfare in Context of Defence Forces in Present Scenario," 2023 Second International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), 2023, pp. 1-6, doi: 10.1109/ICEEICT56924.2023.10157307.
7. R. Khodke and V. N. Dhawas, "Decentralized approach for jamming illegal access and secure data recovery in military networks," 2016 Conference on Advances in Signal Processing (CASP), 2016, pp. 344-349, doi: 10.1109/CASP.2016.7746193.

1053477-3045-1396-24-21

UNMANNED GROUND VEHICLES DEVELOPMENT IN NATO

Artur MACHADO
Lieutenant (OF-1), Master, Portuguese Army, Lisbon, Portugal
E-mail: machado.ajsc@exercito.pt

Alexandra MOUTINHO, PhD.
Professor, IDMEC, Instituto Superior Técnico, Universidade de Lisboa, Lisbon, Portugal

Miguel PINHO
MSc student, Instituto Superior Técnico, Universidade de Lisboa, Lisbon, Portugal

Tiago SILVA
MSc student, Instituto Superior Técnico, Universidade de Lisboa, Lisbon, Portugal

Abstract*: In recent years, society has witnessed an impressive race for Unmanned Ground Vehicles (UGVs) capabilities. The development of UGVs is directly linked to sensors, processors and actuators and can be approached through a modular pipeline consisting of perception, localization, planning, and control, or through an end-to-end pipeline. The applications of UGVs on the battlefield are numerous and of clear interest to NATO, which has motivated several initiatives by member countries for the development and enhancement of this capability.*

Keywords: *Unmanned Ground Vehicle, Autonomous Vehicle, Sensors, Control, Machine Learning, Defence, Autonomy.*

Introduction

In recent years, society has witnessed an impressive race for emerging and disruptive technologies (EDT) such as advanced robotics, artificial intelligence, computer power, and communications that enabled militaries to develop and utilize different-sized Unmanned Ground Vehicles (UGVs) to support a variety of combat and support missions. The market for unmanned ground vehicles (UGV) has expanded significantly since. This can be attributed to the rising application of modern UGVs for a wider variety of defence and security applications (GlobalData, 2023).

UGV, also known as Autonomous vehicle in some applications, is a comprehensive intelligent system that integrates environmental perception, location, navigation, path planning, decision making and motion control (Liu, et al., 2021). UGVs should have customizable models capable of supporting military tactics in combat, Intelligence, Surveillance and Reconnaissance (ISR), Logistics, and Explosives and Mine Disposal situations. Such capabilities have motivated nations and organizations such as the United States, European Union, Russia, the United Kingdom, Ukraine, Portugal, among others, to invest large amounts of resources to develop UGVs, and NATO to reference UGVs as one of the key technologies by 2035 (NATO Science & Technology Organization, 2020; GlobalData, 2023).

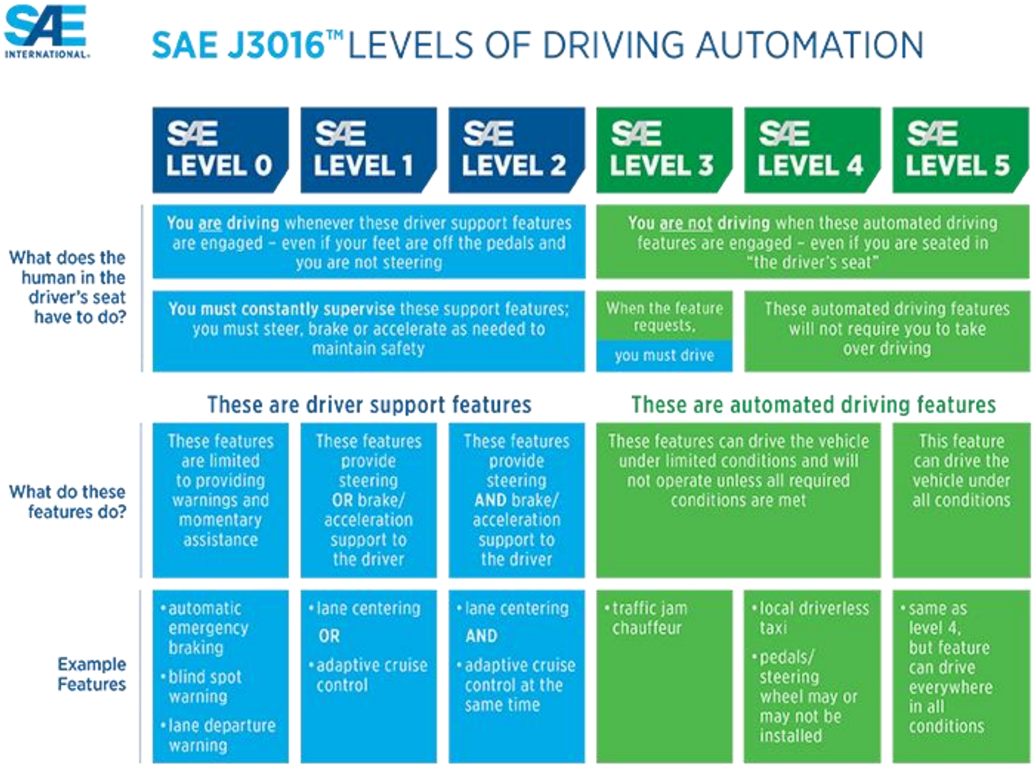
I. Level of autonomy of UGVs

Research in UGVs is very vast due to their broad functions and applications, but also due to the great evolution they have undergone in recent years. However, definitions are beginning to be agreed upon to establish development baselines. It is crucial to elucidate certain taxonomy and definitions concerning unmanned ground vehicles to facilitate comparison among different solutions. The most recent classifications include the "SAE J3016 - Levels of Driving Automation" by the Society of Automotive Engineers and the Concept For Robotic and Autonomous Systems by the Australian Defence Force.

1.1 SAE J3016

The SAEJ3016 delineates motor vehicle driving automation systems on roads that execute part or all of the dynamic driving tasks consistently. It furnishes a taxonomy with comprehensive definitions for six levels of driving automation, spanning from no driving automation (Level 0) to full driving automation (Level 5) (SAE International, 2021):

- Level 0 - No Driving Automation;
- Level 1 - Driver Assistance;
- Level 2 - Partial Driving Automation;
- Level 3 - Conditional Driving Automation;
- Level 4 - High Driving Automation;
- Level 5 - Full Driving Automation.



SAE INTERNATIONAL

SAE J3016™ LEVELS OF DRIVING AUTOMATION

	SAE LEVEL 0	SAE LEVEL 1	SAE LEVEL 2	SAE LEVEL 3	SAE LEVEL 4	SAE LEVEL 5
What does the human in the driver's seat have to do?	You are driving whenever these driver support features are engaged – even if your feet are off the pedals and you are not steering			You are not driving when these automated driving features are engaged – even if you are seated in "the driver's seat"		
	You must constantly supervise these support features; you must steer, brake or accelerate as needed to maintain safety			When the feature requests, you must drive	These automated driving features will not require you to take over driving	
	These are driver support features			These are automated driving features		
What do these features do?	These features are limited to providing warnings and momentary assistance	These features provide steering OR brake/ acceleration support to the driver	These features provide steering AND brake/ acceleration support to the driver	These features can drive the vehicle under limited conditions and will not operate unless all required conditions are met		This feature can drive the vehicle under all conditions
Example Features	• automatic emergency braking • blind spot warning • lane departure warning	• lane centering OR • adaptive cruise control	• lane centering AND • adaptive cruise control at the same time	• traffic jam chauffeur	• local driverless taxi • pedals/ steering wheel may or may not be installed	• same as level 4, but feature can drive everywhere in all conditions

Figure no. 6. SAE J3016 Levels of driving automation. From SAE International, 2021.

The Fig. 1 explains the differences between the levels based on the actions of the drivers and their features

1.2 Australian Defence Force's categorisation

Australian Defence Force published its concept for Robotic and Autonomous Systems in 2020 and defined a classification based on Control Context and Technical Context, building upon the classifications discussed in Williams & Scharre, 2017 (Australian Defence Force, 2020). This classification is based on four stages of human-system interaction:

- Full human control: In this scenario, a human oversees every aspect of the system's operation, either directly through physical interaction, or via remote control;
- Human in the loop: The system autonomously executes certain functions but relies on human intervention to fulfill tasks that complete the system's operational cycle;
- Human on the loop: In this scenario, the system autonomously executes all functions, yet a human retains the ability to intervene to halt or adjust the outcome before the task reaches competition;
- Human starts the loop: In this case, a human establishes the operational parameters and triggers the system's operation; thereafter, the machine operates independently, requiring no additional human interaction to finalize the task.

Through this context, systems are classified into four categories regarding their autonomy (The Australian Army, 2022):

- Remote systems: These systems are operated by humans through remote methods. Devoid of the remote control element, these systems possess minimal ability to function autonomously;
- Automatic Systems: These systems are pre-programmed to react to stimuli based on rules, following a deterministic approach. They can accomplish their tasks without additional human intervention;
- Autonomic Systems: Such systems execute tasks defined by humans by adhering to a set of predefined guidelines and responding to stimuli in a probabilistic fashion. Autonomic systems may require human input to fulfill their function or operate without further supervision;
- Autonomous systems: These systems ascertain the methods required to accomplish predefined goals. Responding to stimuli in a probabilistic manner, an autonomous system can adapt its task execution methods accordingly to the final goal.

II. Pipeline for UGV Development

The inherent complexities associated with developing and operating UGVs in comparison to Unmanned Aerial Vehicles (UAVs) and Unmanned Surface Vehicles (USVs) led to severely restricted operational capabilities for UGV platforms until 2015. However, significant advancements in UGV key-technologies have been achieved over the past years. Progress in semi-autonomous navigation and solutions enhancing terrain adaptability have notably enhanced the capabilities of current UGV platforms (GlobalData, 2023). In the realm of autonomous driving, two primary paradigms emerge: the modular pipeline and the end-to-end approach (Fig. 2).

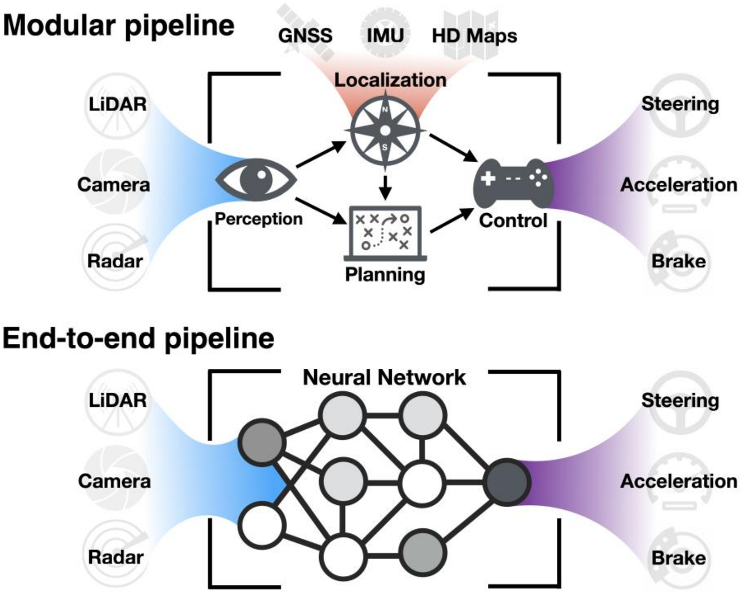


Figure no. 2. A typical autonomous vehicle system overview, highlighting core competencies. From Pendleton, et al., 2017

The modular pipeline delineates a framework comprised of interconnected modules, each fulfilling distinct functions within the broader system. Conversely, the end-to-end approach perceives the entire pipeline as a singular, learnable machine learning task, thereby bypassing discrete modular segmentation. These contrasting methodologies epitomize divergent strategies in the development and implementation of autonomous driving systems, each bearing implications for system architecture, adaptability, and performance optimization (Tampuu, et al., 2021).

2.1 Sensors

Sensors data collection is the premise for the next phases of the UGVs operation. To achieve good data collection, it is necessary to have adequate sensors capable of collecting all the necessary information. LiDAR, RADAR, RGB camera, Infrared camera are the most common sensors. LiDAR and RADAR can measure the distance to an object and allow the creation of a real-time 3D map of the environment, which is useful information for obstacle detection, while cameras are fundamental to understanding the surrounding environment (Vargas, Alsweiss, Toker, Razdan Rahul, & Santos, 2021).

Light Detection and Ranging (LiDAR) employs laser beams for the transmission and reception of data, facilitating the determination of object position, orientation, and velocity through time differential calculations. The data collected takes the form of a series of 3D point coordinates, constituting a point cloud relative to the LiDAR's coordinate center, alongside echo intensity measurements. LiDAR systems offer comprehensive, omni-directional detection capabilities and are categorized into single-line and multi-line variants based on laser beam count. Single-line LiDAR provides two-dimensional target information, while multi-line LiDAR captures three-dimensional data (Liu, et al., 2021). LiDAR boasts extensive detection ranges and wide fields of view, ensuring high data precision and depth acquisition irrespective of lighting conditions. However, Lidar systems are large in size and prohibitively expensive; they lack the ability to capture target color and texture information, and feature low angular resolutions. Long-distance point clouds often exhibit sparse distributions, leading to potential misdetection and missed detection issues, compounded by susceptibility to environmental factors such as rain, snow, fog, and sandstorms. Moreover, LiDAR's active sensing nature, involving self-emitted laser beams for detection, compromises its concealment, particularly in military applications (Liu, et al., 2021).

RADAR transmits radio waves, which bounce off objects in the environment and return to the radar sensor. It provides information about the objects' position, distance, and speed based on the time it takes, utilizing the Doppler property (Matos et al., 2023). In UGVs, the radar is primarily utilized for object detection and tracking, blind-spot detection, lane change assistance, collision warning, and other Advanced Driver Assistance Systems (ADAS)-related functions (Rosique et al., 2019; Matos et al., 2023). Radar waves offer higher penetrability and perform well in all weather conditions, accurately detecting short-range targets in various directions around a vehicle. Nevertheless, radar sensors have limitations such as reduced precision, a limited Field of View, and the potential for false positives due to signal bouncing (Rosique, et al., 2019)

RGB cameras, also referred to as visible light cameras, produce images by capturing and recording the visible light reflecting off objects in the scene. These cameras operate within the same wavelength range as the human eye, typically between 400 and 780 nanometers, and are divided into three color bands: Red, Green, and Blue (RGB). To achieve stereoscopic vision, two visible light cameras with known focal lengths are combined to generate a new channel containing depth (D) information. This capability allows the camera (RGBD) to capture a three-dimensional image of the surroundings around the vehicle (Ahangar, et al., 2021).

Infrared cameras gather environmental data by detecting signals of infrared radiation emitted by objects. They serve as valuable complements to traditional cameras and are commonly employed in environments with intense illumination, such as vehicles exiting tunnels and facing direct sunlight, or for the detection of hot bodies, particularly during nighttime operations (Rosique, et al., 2019; Liu, et al., 2021). Due to sensor limits, redundancy and complementarity of sensors is required, which implies cross-referencing information from different sensors (Hu, et al., 2020). Asynchronous multi-sensor-based data fusion methods have attracted considerable attention for harsh environments, but the capability of operation is not enough to deal with multiple asynchronous heterogeneous real-time sensors (Hu, et al., 2020).

2.2 Perception

Simultaneous Localisation and Mapping (SLAM) is a common technique in the field of mobile robots, and researchers have put a noticeable effort into adjusting the algorithms to suit UGV applications (Takleh et al., 2018). SLAM algorithms combine a set of sensors to build a map of the UGVs surroundings while simultaneously keeping track the vehicle’s current position in reference to the built map (Takleh, et al., 2018). This technique usually implements vision-based sensors, but other sensors such as GPS, LiDAR, and SONAR have also been used to improve their accuracy.

Deep learning approaches have shown great improvements in image detection and classification. Matos, et al., 2023 developed an algorithm for detecting and classifying civilian/military and armed/unarmed individuals through the fusion of an RGB camera and FLIR thermal camera based on the You Only Look Once v8 (YOLOv8) algorithm. Examples of results of this algorithm can be seen in Fig. 3. In Figure 3a), the person on the left is detected by the RGB camera, the person in the middle is detected only by the thermal camera, and the person on the right is detected by both cameras. In Figure 3b), we can see the result of the Military/Civilian classifier.

a) Urban scenario b) Forest scenario

Figure no. 3. People Detection and Classification from Multi-Modal Sensors for Military Purposes. From Matos, et al., 2023

2.3 Localization

Localization can be defined as estimating the vehicle's pose (position, orientation) along with the associated uncertainty in a reference frame (Kumar & Muhammad, 2023). The efficacy of intelligent functionalities within an UGV, such as collision avoidance, hinges upon the attainment of real-time self-localization at the millisecond level and accuracy at the centimetre level (5G-PPP, 2015).

Lidar-, vision-, and data fusion-based localization techniques exhibit promise in fulfilling the accuracy criterion (<30cm) essential UGV operations (5G-PPP, 2015). Lidar-based methodologies have demonstrated superior positioning accuracy in comparison to alternative sensor-based approaches, with disparate lidar-based techniques yielding analogous position accuracies (Liu, et al., 2021). While vision-based localization holds potential for achieving precise vehicle positioning, it may necessitate GPU acceleration to handle substantial image data, and the reliability of cameras under suboptimal illumination or inclement weather conditions warrants further scrutiny. Vehicle-to-Everything (V2X) techniques present a cost-effective solution for UGV localization across a broad spectrum of signal intensities and Vehicular ad hoc network (VANET) coverage. Nonetheless, mitigating the challenges of signal latency and packet loss within V2X systems is imperative to enhance localization accuracy and consistency. It is evident that no singular sensor can fully satisfy all localization prerequisites for autonomous driving. Consequently, data fusion-based methodologies emerge as a focal point in research endeavours aimed at achieving cost-effective self-localization for UGVs, outpacing other single sensor-based approaches (Liu, et al., 2021).

2.4 Planning

In the realm of autonomous systems, planning encompasses both global route planning and local path planning. The global planner's task is to determine the most efficient route from the starting point to the destination, typically relying on GPS and offline. Meanwhile, the local planner aims to execute the global plan by identifying obstacle-free trajectories within the configuration space between the initial and final points (Yurtsever, et al., 2020)

Various algorithms such as A* search and hierarchical techniques like Rapidly-exploring Random Trees (RRT) are commonly employed for global planning (LaValle & Kuffner, Jr, 2001). While A* search is known for its accuracy, it tends to be slower and can yield jerky trajectories (Bautista, 2017; Yurtsever, et al., 2020). Conversely, RRT offers a faster solution but may also result in erratic paths (Yurtsever et al., 2020). Local planning plays a critical role in ensuring the safe implementation of global plans. Graph-based planners, exemplified by the A* method, generate discrete paths, whereas state lattice algorithms are adept at handling high-dimensional spaces albeit with a high computational load (Pivtoraiko & Kelly, 2005). The integration of Deep Learning (DL) and Reinforcement Learning (RL) marks a burgeoning trend in local planning, leveraging Convolutional Neural Networks (CNNs) to generate paths from sensory data such as LiDAR inputs (Yurtsever, et al., 2020).

2.5 Control and chassis

The control module, positioned as a pivotal component, interfaces with the decision and planning module, assimilating information and executing a spectrum of functions pertinent to the physical manipulation of UGV, encompassing steering, braking, acceleration, among others (Yurtsever, et al., 2020). Constituting the ultimate stage, the chassis orchestrates the interface with an array of mechanical constituents affixed onto its structure, comprising the accelerator pedal motor, brake pedal motor, steering wheel motor, and gear motor. This intricate network delineates the nexus between digital directives and the physical infrastructure of the UGV, embodying the symbiotic relationship between computation and mechanics (Yurtsever, et al., 2020).

In recent years, there has been a major evolution in X-by-wire technology. This enables a significant increase in chassis performance in terms of mobility. Subsystems such as steering-by-wire, braking-by-wire, and driving-by-wire replace the mechanical subsystems and allow the integration of sensors and Artificial Intelligence (AI) systems for much more precise control of the vehicle dynamics and a reduction of weight and volume (Nl et al., 2018).

2.6 End-to-end approach

The end-to-end driving approach represents a burgeoning trend in UGV research. It proposes a unified machine learning approach to optimize the entire driving pipeline, from processing sensory inputs to generating steering and acceleration commands. Unlike modular systems, end-to-end architectures treat the driving task as a single learning task, allowing models to autonomously learn optimal representations without predefined information bottlenecks. This approach offers flexibility in decision-making and potential solutions for complex driving scenarios, such as low-light conditions, through implicit reasoning. However, it requires ample expert driving data or extensive exploration and training in Reinforcement Learning. Imitation Learning and Reinforcement Learning stands as the prevailing strategies within the domain of end-to-end methodologies (Tampuu, et al., 2021).

III. The Present of UGVs in NATO

3.1 Applications for UGV in NATO Eastern Battlegroups

Due to the Euro-Atlantic instability and Russia's aggressive actions against Ukraine, the NATO alliance reinforced its eastern flank with 8 battlegroups. These battlegroups aim to ensure the necessary readiness and responsiveness, and UGVs offer multifaceted applications for bolstering defence strategies, from efficient logistics to perimeter security, autonomous patrols in vulnerable areas, reconnaissance and surveillance of terrains, and even urban incursions and opening operations.

In the logistics domain, UGVs make logistics operations more agile and effective. In high-risk areas, such vehicles conduct autonomous patrols, minimizing human exposure to potential threats. Their reconnaissance and surveillance capability is enhanced through advanced sensors, providing crucial real-time information about enemy positions and the characteristics of the surrounding terrain.

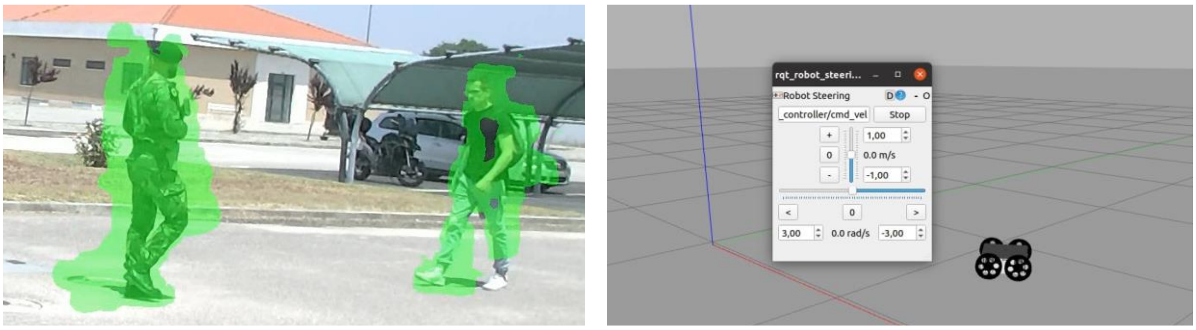
Regarding perimeter security, UGVs play a critical role in the early detection of intrusions, strengthening the defences of operational bases. During urban incursions, these vehicles operate in partnership with infantry units, facilitating penetration into hostile environments. In opening operations, their use is vital in creating safe passages through minefields or natural barriers.

3.2 NATO's nations initiatives

Through the European Commission, the recent iMUGS project launched in 2020 has propelled the development of an Autonomous Driving Kit for ground vehicles. The project aimed to construct a modular and scalable framework for hybrid manned-unmanned systems, catering to a diverse array of missions while facilitating seamless updates or alterations to assets and functionalities across the system (European Commission, n.d.). This includes aerial and ground platforms, command, control, and communication apparatus, sensors, payloads, and algorithms. This project involved 14 entities from 7 member countries.

The Defense Advanced Research Projects Agency (DARPA) launched the Robotic Autonomy in Complex Environments with Resiliency (RACER) program to develop algorithms for autonomous combat vehicles that can match or exceed the driving capabilities of soldiers. The objectives of the RACER program include not only autonomous algorithms but also the creation of simulation environments that will support the rapid advancement of autonomous driving capabilities for future UGVs.

Portugal, through the Portuguese Army in partnership with Instituto Superior Técnico, launched the EXE03 – Unmanned Ground Vehicle (UGV), which encompasses two work packages – UGVSecurity and eMOVE. The UGVSecurity aims to develop a transportable UGV for active security of critical infrastructures and/or detection of objects interest (Fig. 4 and 7). The eMOVE consists of adapting the M113 APC platform into a UGV, specifically in electrifying the powertrain and integrating an Autonomous Driving Kit (ADK).



a) Movement detected (green) in daytime scenario with RGB.

b) Representation of the UGVSecurity robot in Gazebo.

Figure no. 4. UGVSecurity project outcomes

Conclusions

Since 2015, developments have created a growing trend of interest in UGVs, which has consequently led to accelerated development of key technologies. Sensors can cover the entire environment and collect all necessary data, although they still face some unresolved challenges, such as the need for sensor complementarity and synchronization of data from different sensors. Perception, localization, planning, and control methods are becoming increasingly robust, and the focus on machine learning combined with increased computing power has allowed for new approaches and the overcoming of some challenges that deterministic methods face.

UGVs play a crucial role in modernizing and optimizing military operations, offering substantial advantages across a wide spectrum of operational scenarios and enabling NATO to achieve high standards of readiness and responsiveness. The current investment by various entities within the NATO alliance demonstrates their real interest and paves the way for significant developments in the coming years. UGVs represent a path of no return.

BIBLIOGRAPHY:

1. 5G-PPP, 2015. *5G Automotive Vision [Online],* s.l.: s.n (In-text citation: 5G-PPP, 2015).
2. Ahangar, M. N., Ahmed, Q., Khan, F. & Haffez, M., 2021. A Survey of Autonomous Vehicles: Enabling Communication. (In-text citation: Ahangar, et al., 2021).
3. Australian Defence Force, 2020. *Concept for Robotic and Autonomous Systems.* s.l.:s.n. (In-text citation: Australian Defence Force, 2020).
4. Baghdadi, N. & Zribi, M., 2016. *Optical Remote Sensing of Land Surface. Techniques and Methods.* s.l.:ISTE Press - Elsevier, Year: 2016. (In-text citation: Baghdadi & Zribi, 2016).
5. Bautista, D. G., 2017. *Functional architecture for automated vehicles trajectory planning in complex environments,* s.l.: Université Paris sciences et lettres. (In-text citation: Bautista, 2017).
6. Bienzeisler, J., Cousin, C., Deschamps, V. & Eberle, U., 2017. *Automated Driving Applications and Technologies: Legal Aspects on Automated Driving,* s.l.: s.n. (In-text citation: Bienzeisler, et al., 2017).
7. European Comission, n.d. *iMUGS.* s.l.:s.n. (In-text citation: European Comission, s.d.).
8. GlobalData, 2023. *Unmanned Ground Vehicles - Thematic Intelligence,* s.l.: s.n. (In-text citation: GlobalData, 2023).
9. Hu, J.-w.et al., 2020. Asurvey onmulti-sensor fusion based obstacle detection for intelligent ground vehicles in off-road environments. (In-text citation: Hu, et al., 2020).
10. Kumar, D. & Muhammad, N., 2023. A Survey on Localization for Autonomous Vehicles. *IEEEAccess*. (In-text citation: Kumar & Muhammad, 2023).
11. LaValle, S. M. & Kuffner, Jr, J. J., 2001. Randomized Kinodynamic Planning. *The International Journal of Robotics Research*. (In-text citation: LaValle & Kuffner, Jr, 2001).
12. Liu, Q. et al., 2021. Review on Vehicle Detection Technology for Unmanned. *Sensors 2021*. (In-text citation: LaValle & Kuffner, Jr, 2001).
13. Matos, J., Moutinho, A. & Machado, A., 2023. People Detection and Classification from Multi-Modal Sensors for Military Purposes. (In-text citation: Liu, et al., 2021).
14. NATO, 2023. *NATO's military presence in the east of the Alliance.* [Online] [Accessed https://www.nato.int/cps/fr/natohq/topics_136388.htm?selectedLocale=en february 2024]. (In-text citation: (NATO, 2023).
15. Nl, J., Hu, J. & Xiang, C., 2018. Design and Advanced Robust Chassis Dynamics Control for X-by-Wire Unmanned Ground Vehicle. *Synthesis Lectures on Advances in Automotive Technology 2(1):i-130*. (In-text citation: Nl, et al., 2018).
16. Pendleton, S. D. et al., 2017. *Perception, Planning, Control and Coordination for Autonomous Vehicles,* s.l.: s.n. (In-text citation: Pendleton, et al., 2017).
17. Pivtoraiko, M. & Kelly, A., 2005. Efficient constrained path planning via search in state lattices. *Proceedings of 8th International Symposium on Artificial Intelligence, Robotics and Automation in Space (iSAIRAS '05).* (In-text citation: Pivtoraiko & Kelly, 2005).
18. Rosique, F., Navarro, P., Fernández, C. & Padilla, A., 2019. A Systematic Review of Perception System and Simulators for Autonomous Vehicles Research. *Sensors*. (In-text citation: Rosique, et al., 2019).
19. SAE International, 2021. *SAE Levels of Driving Automation™ Refined for Clarity and International Audience.* [Online] Available at: https://www.sae.org/blog/sae-j3016-update [Accessed 12 February 2024]. (In-text citation: SAE International, 2021).
20. Takleh, T. T. O. et al., 2018. *A Brief Survey on SLAM Methods in Autonomous Vehicle,* s.l.: International Journal of Engineering & Technology. (In-text citation: Takleh, et al., 2018).
21. Tampuu, A. et al., 2021. A Survey of End-to-End Driving:. (In-text citation: Tampuu, et al., 2021).

22. The Australian Army, 2022. *Robotic & Autonomous Systems Strategy v2.0.* s.l.:s.n. (In-text citation: The Australian Army, 2022).
23. Williams, A. & Scharre, P., 2017. *Autonomous Systems – Issues for Defence Policymakers,* s.l.: NATO – Allied Command Transformation. (In-text citation: Williams & Scharre, 2017).
24. Yurtsever, E., Lambert, J., Carballo, A. & Takeda, K., 2020. A Survey of Autonomous Driving: Common Practices and Emerging Technologies. (In-text citation: Yurtsever, et al., 2020).

1053477-3045-1396-24-22

SYSTEMATIC ACTIONS EXECUTED WITH UNDERWATER DRONES IN THE BLACK SEA

Alin DOGARU
master degree student, the Naval Forces Department, the Command and Staff Faculty,
"Carol I" National Defence University, Bucharest, Romania
E-mail: ing_dogy@yahoo.com

Marius MĂNĂILĂ
master degree student, the Naval Forces Department, the Command and Staff Faculty,
"Carol I" National Defence University, Bucharest, Romania
E-mail: mana12mar@yahoo.com

***Abstract**: In the current geopolitical context, the Black Sea has become a high-intensity theater of operations, particularly focusing on the development and deployment of advanced technologies such as underwater drones. These autonomous underwater vehicles are a crucial component in defense and surveillance strategies, offering expanded capabilities for tactical and reconnaissance operations. In this article, I aimed to emphasize the importance of using underwater drones in systematic actions in the Black Sea, these systems being increasingly used in conflicts on a global scale. In order to achieve this approach, we established the identification of the impact of the introduction of a new technology in the underwater field for the detection, interception, and destruction of other underwater combat means. I also want to identify the role of the underwater drone in military actions in the Black Sea. The most recent events in Ukraine, with a major impact on military developments, bring back to attention the situation of developments regarding this new means of combat that goes beyond the military field, entering the wider field of security. Equipping the Naval Forces with underwater drones is a necessity, as they are a new stage of military innovation. The introduction and operation of underwater drones in the Black Sea opens new horizons for maritime security. However, it is essential that these technologies are used under the principles of international law and that their impact on regional stability is taken into account.*

***Keywords**: systematic actions, underwater drone, maritime space, submarine. detection, maritime security.*

Introduction

In this article, I will analyze the technological development of underwater drones, their use in combat, as well as their evolution and military progress. Underwater military drones, also known as unmanned underwater vehicles (UUVs) or autonomous underwater vehicles (AUVs), cover their history, development, types, and primary functions. These sophisticated systems play a crucial role in modern naval operations, providing significant advantages in terms of safety, efficiency, and capabilities.

The underwater drone concept dates back to the Cold War era when initial research focused on underwater surveillance and mine countermeasures. These early designs were primarily remotely operated vehicles (ROVs) tethered to a control source.

Technological advances over the decades, particularly in battery life, propulsion systems, and remote sensing, have led to the development of more autonomous and sophisticated UUVs. The integration of AI and machine learning has further enhanced their operational capabilities.

Types of underwater military drones:

Remotely Operated Vehicles (ROVs): These are tethered to a ship or submarine and are controlled by a remote operator. They are often used for tasks such as body inspections, mine neutralization, and search and recovery missions.

Autonomous Underwater Vehicles (AUVs): AUVs operate independently of a human controller. They are pre-programmed to perform specific tasks such as mapping, surveillance, and reconnaissance. AUVs range from small, portable units to large, complex systems. Hybrid systems: Some newer designs combine the features of ROVs and AUVs, providing greater flexibility and adaptability in various operations.[7]

Primary Functions and Capabilities:

Surveillance and Reconnaissance: UUVs gather critical intelligence by covertly monitoring enemy activity, mapping terrain, and detecting hostile assets.

Mine Countermeasures: They play a key role in the detection, classification, and neutralization of underwater mines, significantly reducing the risk to naval personnel.

Anti-submarine warfare: UUVs help detect and track enemy submarines, contributing to the protective screen around carrier strike groups.

Search and rescue operations: In situations such as downed aircraft or sunken ships, UUVs can reach depths inaccessible to human divers, aiding in search and recovery efforts. The development and deployment of military underwater drones have revolutionized naval warfare and strategy. Offering enhanced capabilities in a variety of undersea tasks, these drones contribute significantly to the safety and effectiveness of naval operations. Their continued evolution, marked by technological advances, promises even greater contributions to military and civilian applications in the future. The significance of military underwater drones in modern military operations cannot be overstated. These sophisticated tools, known as unmanned underwater vehicles (UUVs) or autonomous underwater vehicles (AUVs), have brought about a paradigm shift in the way naval operations are conducted. They provide unique advantages and capabilities that enhance the effectiveness, safety, and scope of military missions. UUVs can operate in hostile or surveillance environments. Their ability to pass undetected by enemy radars or sonars is a significant tactical advantage. Unlike manned submarines or surface ships, UUVs are not limited by human resistance. They can be deployed for long periods, covering vast areas of the sea, which is crucial for surveillance and monitoring missions. UUVs can be used in environments too dangerous for manned vessels, such as heavily mined waters or near hostile forces.

Strategic advantages:

UUVs are essential in intelligence gathering, providing real-time data and high-resolution images of the seabed, enemy installations, or activity. This information is crucial for informed decision-making and strategic planning. UUVs act as force multipliers, allowing navies to conduct multiple operations simultaneously without the need for a proportional increase in personnel or ships. This amplifies naval power and presence. Operating UUVs is generally more cost-effective than deploying large manned vessels for the same tasks. This allows for a more efficient allocation of military resources.

Advances in AI, machine learning, and robotics promise to further improve the capabilities of UUVs. Future developments could include more autonomous decision-making capabilities, integration with other military assets, and advanced stealth technologies. In short, military underwater drones have become indispensable in modern naval operations. Their capabilities

[7] Lucian Valeriu Scipanov, Florin Nistor, ”The timeliness of an underwater sensor system”, SEA – CONF 2019, 5th International Conference, May 17th-18th, Constanța, 2019, „Mircea cel Bătrân” Naval Academy, Vol. XXII, 2019, Issue no. 2, pp. 14-21.

in intelligence gathering, mine countermeasures, and anti-submarine warfare, among other areas, provide significant strategic and tactical advantages. As technology evolves, their role in future maritime operations will expand, further strengthening their importance in global military strategies.

Finally, I propose to strengthen the main idea of my approach regarding the opportunity to develop a capability within the Romanian Naval Forces, through the use of underwater drones in systematic actions to deter threats from aggressor states that intend to destabilize the status quo.

1. Technological developments of military underwater drones

The idea of unmanned underwater vehicles emerged after World War II, primarily driven by military needs for safe and effective means to conduct underwater military action and mine countermeasures.

Early UUVs were tethered submersibles, controlled remotely from a ship or submarine. They have been used mainly for oceanographic research and in the oil and gas industry for the maintenance of subsea infrastructure.

During the Cold War, the strategic value of UUVs became apparent, leading to increased investment in military applications, particularly mine surveillance, reconnaissance, and countermeasures.

The 2000s marked a significant shift towards fully autonomous underwater vehicles. These AUVs could independently perform complex missions based on pre-programmed instructions and advanced algorithms. Recent advances have integrated AI and machine learning into UUV systems, enabling more sophisticated decision-making capabilities, improved navigation, and adaptive mission execution. Modern UUVs range from small, portable units that can be launched manually to large, complex systems capable of extended deep-sea missions. Ongoing research focuses on expanding the operational range and depth capabilities of UUVs, enabling longer missions in more challenging environments. Overcoming the challenge of underwater communication remains a key area of development, with emerging technologies such as underwater acoustic networks.[8]

As advances continue, UUVs are poised to play an increasingly vital role in naval operations. The technical specifications of military underwater drones, also known as unmanned underwater vehicles (UUVs) or autonomous underwater vehicles (AUVs), are diverse and sophisticated. These specifications are crucial because they define the capabilities, limitations, and potential applications of these drones. Key areas of focus are propulsion systems, communication methods, and power sources.

Propulsion systems:

Thrusters and Propellers: Most UUVs use electrically powered thrusters or propellers for propulsion. The design and number of these propulsion units vary depending on the size and purpose of the drone.

Glider Technology: Some AUVs use glider technology, using buoyancy modifications in combination with wings to propel themselves forward. This method is very energy efficient and suitable for long-duration missions.

Jet Propulsion: Rarely, some specialized UUVs use water jet propulsion, similar to some marine animals, for stealth and high-speed operations.

[8] Daniel-Cornel Tănăsescu, Ion Chiorcea, ”Unmanned Underwater Vehicles Technology’s Impact On Combat Situational Awareness”.

Advanced Propulsion: Research into more advanced propulsion methods, such as magnetohydrodynamic propulsion (MHD), offers the potential for quiet operation, a critical feature for stealth in military applications.

Communication methods:

Acoustic Communication: Radio waves underwater are ineffective, so UUVs typically use acoustic signals to communicate. However, this method has limitations in range and data transfer rates.

Surface wireless data transfer: When on the surface, UUVs can switch to radio or satellite communications for high-speed data transfer and to receive complex instructions.

Optical communication: Emerging technologies include underwater optical communication, which offers higher data rates than acoustic methods, but has limited range and requires clean water conditions.

Power sources:

Batteries: Most UUVs are powered by rechargeable batteries. Lithium-ion batteries are common due to their high energy density and efficiency.

Fuel cells: For longer endurance, some advanced UUVs use fuel cells, which can provide greater energy capacity compared to traditional batteries.

External Power Sources: Connected UUVs (ROVs) can draw power from the host vessel, allowing for extended operational times, but at the cost of limited autonomy and mobility.

Energy-harvesting technologies: Research is ongoing into energy-harvesting methods, such as solar power or ocean thermal energy conversion, which could provide a near-infinite range for certain types of missions.

The technical specifications of underwater drones are varied and highly specialized, tailored to meet specific operational needs. Propulsion systems are chosen for efficiency and mission suitability, communication methods are tailored to the challenging underwater environment, and power sources are selected based on the required endurance and power needs of the vehicle. As technology advances, we can expect further innovations in these areas, improving the capabilities and applications of UUVs.

Each type of military underwater drone is designed with specific capabilities and functionality to meet different needs in naval warfare and maritime operations. From the precision and control of ROVs to the independence and endurance of AUVs, these drones significantly enhance the capabilities of naval forces, providing strategic advantages in surveillance, reconnaissance, and combat operations. As technology advances, these vehicles are likely to become even more versatile and integrated into military maritime operations.

2. Tactical use in military operations

Surveillance and reconnaissance are essential functions of military underwater drones, especially in systematic actions. These unmanned underwater vehicles (UUVs), including autonomous underwater vehicles (AUVs) and remotely operated vehicles (ROVs), play a crucial role in gathering critical intelligence in the ASuW and ASW combat environment. Their ability to operate in stealth, remote, or dangerous environments makes them invaluable assets for intelligence gathering and situational awareness.[9]

[9] https://meta-defense.fr, accesed on the date of 15.02.2024.

Applications in systematic actions:

Strategic surveillance: Monitoring foreign naval activities, imposing maritime blockades, and patrolling strategic waterways.

Pre-Mission Intelligence Gathering: Prior to amphibious assaults UUVs can discreetly survey enemy beaches, landing zones, and fortifications.

Anti-submarine warfare: Detection and tracking of enemy submarines, contributing to the defense of naval operational forces and commercial shipping lanes.

Mine Detection and Classification: Locating and identifying mines to ensure the safe passage of military and commercial vessels.

The role of underwater drones in surveillance and reconnaissance is vital in modern military strategy. Their stealthy, sustained, and versatile intelligence-gathering capabilities are unmatched by manned platforms, making them indispensable for a wide range of naval intelligence operations. As technology advances, the scope and effectiveness of these UUVs in reconnaissance roles are expected to increase, further enhancing their strategic value in military operations.

Mine countermeasures are a critical component of naval operations, and underwater drones have become indispensable tools in this field. Unmanned underwater vehicles (UUVs), including autonomous underwater vehicles (AUVs) and remotely operated vehicles (ROVs), are widely used for mine detection and neutralization, increasing the safety and efficiency of maritime operations.

Mine detection:

Sonar systems: Side-scan sonar: Provides high-resolution images of the seabed, enabling mine detection even in crowded underwater environments.

Synthetic Aperture Sonar: Provides enhanced imaging capabilities crucial for mine detection in complex seabed conditions.

Magnetic Anomaly Detectors: Detect changes in the Earth's magnetic field caused by large metallic objects such as mines.

Optical identification: Equipped with cameras to visually confirm and classify detected objects as mines.

Mine neutralization:

ROVs for mine clearance: Once mines are located and identified, ROVs can be deployed to neutralize them. ROVs are often equipped with robotic arms or tools to place explosive charges for mine clearance.

Cutting Anchored Mine Cables: Specialized tools on UUVs can be used to cut the cables of anchored mines, causing them to float to the surface where they can be safely detonated or recovered.

Remote Mine Detonation: The use of controlled explosions to neutralize mines from a safe distance, thereby minimizing the risk to naval personnel and ships.

The use of underwater drones for mine countermeasures represents a significant advance in naval warfare and maritime security. These UUVs not only increase the efficiency of demining operations but also greatly improve the safety of such missions. With ongoing technological advances, the capabilities of these drones in detecting and neutralizing mines are expected to continue to evolve, further strengthening their role as essential tools in naval operations.

Anti-submarine warfare (ASW) is a critical component of naval defense and the role of underwater drones, particularly unmanned underwater vehicles (UUVs) and autonomous underwater vehicles (AUVs), has become increasingly important in detecting and tracking enemy submarines. These advanced technologies provide new capabilities and strategies in the complex field of submarine warfare.[10]

Role in submarine detection and tracking:

Advanced sonar systems: UUVs are equipped with sophisticated sonar systems capable of detecting the acoustic signatures of submarines. These systems include both active sonar, which sends out pulses and listens for echoes, and passive sonar, which silently detects the sounds of other ships.

Monitoring: UUVs can operate stealthily, quietly monitoring enemy movements without revealing their own position. This covert capability is crucial in ASW as it allows intelligence to be gathered without alerting the adversary.

Long-duration missions: AUVs can be deployed for long periods covering vast areas of the ocean. This resistance allows continuous monitoring and patrolling of strategic areas, choke points, and known submarine routes.

Depth and maneuverability: UUVs can operate at various depths, including those that are difficult for surface ships and manned submarines. Their maneuverability allows them to navigate complex underwater terrain, increasing their effectiveness in detecting submarines.

Integration in systematic actions:

Collaboration with surface vessels and submarines: UUVs often work in tandem with manned surface vessels and submarines, providing them with real-time data. This collaborative approach enhances the overall ASW strategy by combining the strengths of different assets.

Data relay and communication: UUVs can act as communication relays, relaying data between undersea assets and surface command centers. This role is vital in maintaining situational awareness and coordinating ASW efforts.

Deployment from various platforms: UUVs can be launched from surface ships, submarines, and even aircraft, providing flexibility in their deployment and expanding their operational range.[11]

The integration of UUVs into anti-submarine warfare has profoundly transformed naval defense strategies. By improving detection capabilities, expanding operational resilience, and enabling covert and covert operations, underwater drones have become invaluable in countering underwater threats. As technology advances, these UUVs will continue to play a critical role in ensuring maritime security and enhancing naval capabilities in ASW operations.

Covert operations are a critical aspect of military strategy, where stealth and secrecy are paramount. In this context, underwater drones, including unmanned underwater vehicles (UUVs) and autonomous underwater vehicles (AUVs), have emerged as valuable assets. They are uniquely suited to deliver payloads or covertly perform specialized tasks due to their discrete operational capabilities.

Undersea drones play an increasingly vital role in naval operations, capable of delivering payloads and performing specialized tasks with a high degree of stealth and efficiency. As technology advances, their capabilities in covert operations are expected to expand, further increasing their strategic value in military operations where discretion and precision are crucial.

[10] https://www.rumaniamilitary.ro, accesed on the date of 15.02.2024.
[11] https://monitorulapararii.ro, accesed on the date of 15.02.2024.

3. NATO Trends and Romania's Interest in Underwater Drones in the Black Sea

In recent years, NATO has witnessed a significant evolution in military technology, with a particular focus on underwater drones. These technological innovations not only reshaped defense strategies but also provided new opportunities for member states, including Romania, to strengthen their security in areas of strategic interest, such as the Black Sea.

The Black Sea has always been an area of strategic importance, serving as a connecting point between Europe, Asia, and the Middle East. In the context of recent geopolitical tensions, including the increased military activities of the Russian Federation, NATO has intensified its monitoring and defense efforts in this region. Romania, having a key position within the alliance and an extensive border with the Black Sea, has become a central actor in these strategies.

The field of underwater drone development is rapidly evolving, driven by technological advances and increasing demands for sophisticated maritime capabilities. Emerging technologies in this field are improving the functionality, efficiency, and potential applications of underwater drones. Here are some of the key emerging technologies:

Artificial Intelligence and Machine Learning:

Autonomous decision-making: AI and machine learning enable UUVs to make independent decisions based on environmental data and mission objectives, reducing the need for human intervention.[12]

Pattern recognition: Advanced algorithms allow drones to recognize patterns in data, crucial for tasks such as identifying mines or enemy submarines.

Advanced propulsion systems:

Magnetohydrodynamic Propulsion (MHD): This technology, which propels vehicles using magnetic fields and electrically conductive fluids, provides near-silent operation, a critical feature for stealth missions.

Bio-inspired propulsion: Mimicking marine animals, such as the undulating motion of a ray or the jet propulsion of a squid, to improve maneuverability and efficiency.

Energy efficiency and energy sources:

Fuel Cell Technology: Provides longer endurance and autonomy compared to traditional batteries, enabling extended missions without the need for recharging.

Improved communication and data transfer:

Undersea Acoustic Networks: Improving communication capabilities between UUVs and between UUVs and ships or surface stations.

Optical communication: Provides higher data rates than acoustic methods is useful for transmitting large amounts of data, although limited in range, and requires clean water conditions.

Emerging technologies in underwater drone development are pushing the limits of what these sophisticated machines can achieve. From improved autonomy and propulsion to advanced communication and detection capabilities, these innovations open up new possibilities for military applications.

The role of artificial intelligence (AI) and machine learning (ML) in the field of underwater drones or unmanned underwater vehicles (UUVs) and autonomous underwater vehicles (AUVs) is essential in improving their capabilities, autonomy, and operational efficiency. AI and ML technologies are rapidly transforming the way these vehicles perform various tasks, from data analysis to decision-making processes.

[12] https://www.defenseromania.ro, accesed on the date of 15.02.2024.

Integrating underwater drone technology into NATO's strategies is an important step toward modernizing the alliance's defenses. For Romania, this is a crucial moment to assert its position and contribute significantly to stability and security in the Black Sea. Through collaboration and innovation, NATO and Romania can navigate the challenges of the 21st century together, strengthening their defense and security in the face of an ever-changing geopolitical landscape. The integration of AI and ML into underwater drone technology represents a significant leap forward in their evolution. These technologies not only increase the capabilities of UUVs and AUVs, but also open up new possibilities for their military application.

Conclusions

Following the analysis carried out in this article, I believe that this new type of threat can significantly influence military actions, with the Naval Forces having a new set of challenges when it comes to countering drone threats. Ships operate in a complex and dynamic environment with constantly changing weather conditions, sea states, and other factors that can affect the performance of detection and intercepting systems

The accuracy of drones is another important factor, as it allows them to hit targets with great accuracy. Drones can be fitted with sighting and trajectory control systems that allow them to execute attacks with high precision. In addition, drones can be equipped with sensors and video cameras to monitor areas of interest and identify potential targets.

Military underwater drones are a field marked by rapid technological advances and growing strategic importance. These systems enhance operational capabilities in numerous ways, from conducting detailed surveillance to performing high-risk undersea tasks. Looking ahead, the integration of AI, advanced propulsion systems, and energy efficiency is set to further revolutionize their capabilities, making them even more indispensable in both military and civilian applications. As technology advances, the potential for underwater drones continues to expand, opening new frontiers in underwater operations and exploration.

The field of military underwater drones, including unmanned underwater vehicles (UUVs) and autonomous underwater vehicles (AUVs), offers several promising areas for future research. These areas not only aim to improve the capabilities and efficiency of these drones but also to expand their applications in both the military and civilian spheres. These areas for future research aim not only to push the technological limits of military underwater drones, but also to address operational, environmental, and strategic challenges. Continued development in these areas will significantly improve the capabilities of UUVs and expand their roles in military operations, shaping the future of submarine operations.

I believe that this article can analyze the possibility of developing a new capability for carrying out systematic actions in the Black Sea to deter hostile actions against our country, and the Naval Forces equipped with submarine drones can defend the maritime area of responsibility.

BIBLIOGRAPHY:

1. Scipanov Lucian, FLUVIAL FORCES: The Core of Riverine Capabilities, Military Publishing House, Bucharest, 2020.
2. Scipanov Lucian Valeriu, Nistor Florin, *The timeliness of an underwater sensor system,* SEA – CONF 2019, 5th International Conference, May 17th-18th, Constanța, 2019, „Mircea cel Bătrân, Naval Academy, Vol. XXII, 2019.
3. Daniel-Cornel Tănăsescu, Ion Chiorcea, *Unmanned Underwater Vehicles Technology's Impact On Combat Situational Awareness*, Bulletin of the "Carol I" National Defense University.
4. Marinescu Cornel, Defending Romania's Interests on the Danube, National Defense University "Carol I" Publishing House, Bucharest, 2007.
5. https://www. epoca războaielor dronelor aeriene s-a instalat definitiv? | Monitorul Apărării și Securității (monitorulapararii.ro)
6. https://www. meta-defense.fr
7. https://www. fortele –navale.ro
8. https://www. navy.mil

1053477-3045-1396-24-23

ANALYSIS OF SUBMARINE OPERATIONS IN SEMI-ENCLOSED SEAS – THE BLACK SEA

Marian-Vasile SAVA
LTJG, engineer, Military Science PhD candidate, Chief of the Operational Support
Department at 243rd ”Callatis” Radiolocation and Observation Brigade,
Romanian Naval Forces, Constanța, Romania
E-mail: vasile.sava@navy.ro

Abstract: *The article examines the physical-geographical and military peculiarities of semi-enclosed seas, with the goal of analyzing the impact of these characteristics on the use of submarines. It will be demonstrated that their mode of operation is influenced by the specific features of this zone. The study addresses the following objectives: identification and analysis of the characteristics of a semi-enclosed sea from a physical-geographical, military, and human activities perspective, along with a brief analysis of their impact on the operation of submarine platforms in the Black Sea. The first part of the paper highlights the characteristics of a semi-enclosed sea, which are relevant to underwater operations. The second part emphasizes how physical-geographical, military characteristics, and human activities in semi-enclosed seas impact submarine operations. Certain characteristics of submarines suitable for operations in such areas are identified. The novelty of this article lies in the identification of the connection between semi-enclosed seas and the operating mode of submarines; additionally, it identifies technical and operational requirements for submarines that it would be opportune for the Romanian Navy to acquire.*

Keywords: *characteristics of the Black Sea, semi-enclosed seas, submarine operations, operational requirements, underwater operations.*

Introduction

Characteristics of a semi-enclosed sea are crucial for the planning and execution of military actions, as environmental constraints can complicate the planning process or hinder the execution of actions. Additionally, being a space surrounded by land, the effort will be concentrated, and the pace of actions will be high. Semi-enclosed seas, such as the Black Sea, the Baltic Sea, and others, are partially surrounded by land but they have an opening to an ocean or another sea. This can be characterized by a narrow entrance and is often associated with distinct geographic and oceanographic features.

For approaching the study, the following objectives were proposed: identifying and analyzing the characteristics of a semi-enclosed sea relevant to submarine operations and conducting a brief analysis of their impact on the operation of submarine platforms in the Black Sea.

Through analysis and study of specialized works, the first part of the paper focuses on highlighting the characteristics of a semi-enclosed sea. Those features relevant to submarine operations will be emphasized. For this purpose, I have proposed three criteria for analysis: physical-geographical, military, and human activity perspectives.

The second part of the paper highlights how the characteristics of a semi-enclosed sea influence the operational dynamics of submarines. I have also outlined how submarines must adapt their operations in such areas. In this context, I have identified some operational requirements for submarines suitable for operations in such areas, such as the Black Sea.

The novelty of the article lies primarily in identifying the connection between the characteristics of semi-enclosed seas and the operational mode of submarines. Secondly, it involves identifying operational requirements for submarines that the Romanian Naval Forces should consider acquiring.

I. Characteristics of the semi-enclosed sea

Semi-enclosed seas are bodies of water partially surrounded by land, islands, peninsulas, or land barriers, but they maintain connections with oceans or open seas through channels, straits, or gulfs. These seas exhibit intermediate characteristics between open seas and completely enclosed seas (such as inland seas).

To identify relevant features, I proposed an analysis of semi-enclosed seas from three perspectives: physical-geographic, military, and human activities. By employing these analytical criteria, I conducted a brief examination of these areas, identifying features pertinent to the objectives outlined in this article.

1.1 Physical-geographic particularities

Semi-enclosed seas exhibit distinct physical-geographic characteristics compared to open seas or oceans. Several noteworthy features include limited openness, variability in depth and topography, specific marine currents, physical properties of water, and climate.

– Limited openness: Semi-enclosed seas are partially surrounded by land and have a restricted opening to the ocean or another sea. These seas often include narrow entrances, straits, or channels connecting them to a larger sea or ocean.

– Variability in depth and topography: The depth of semi-enclosed seas can vary significantly, ranging from deep areas to shallower zones. This variability can impact water circulation and oceanographic dynamics. Generally, semi-enclosed seas are characterized by shallow waters, with greater depths typically found in the central parts. The seafloor of these seas is generally flat, but mountainous formations may occur in the center. In comparison to open seas or oceans, depths in semi-enclosed seas are considerably smaller.

– Marine currents: Unique marine currents are predominant in semi-enclosed seas, typically following the specific shape of the sea and influenced by its entrances or straits. The presence of peninsulas or islands can also influence current directions. Circular currents are common in semi-enclosed seas, encompassing both surface and deep currents. In comparison to open seas or oceans, semi-enclosed seas tend to have a higher density of currents within their spatial confines.

– Physical properties of water: characteristics such as water salinity and temperature can vary based on local conditions and the degree of connectivity with larger oceans or freshwater inflows from rivers. Homogeneity levels may be lower near river estuaries. Generally, the salinity in semi-enclosed seas is lower than that in oceans or open seas.

– Climate impact: due to their smaller size, semi-enclosed seas may be more sensitive to climate changes, experiencing rapid fluctuations in water temperature or sea level. These seas can be subject to specific local weather conditions, such as frequent storms or fogs, which can affect navigation and the marine environment. Compared to oceans, the weather in semi-enclosed seas is more variable across their surface.

Later in the article, we will explore how the distinctive features of semi-enclosed seas wield a profound impact on underwater operations. An understanding of these factors is crucial when discussing the planning and execution of submarine operations.

1.2 Human Activities

Semi-enclosed seas have been key locations for diverse human activities throughout history. These seas represent strategic points for their coastal states as they offer opportunities for economic development. Human activities in these areas include trade and maritime transport, fishing, tourism, and energy exploration.

– Trade and maritime transport: semi-enclosed seas are often traversed by important maritime routes, facilitating trade and maritime traffic between different regions of the world. The ports in these seas are essential for global maritime transport. Generally, commercial routes in these seas are crowded due to spatial considerations and accessibility in such areas. Areas near straits are particularly congested, and commercial vessels can be found anchored off ports.

– Fishing: these seas provide significant resources for commercial fishing. Fish and other marine organisms in these areas are exploited to meet the dietary needs of local communities and the fishing industry. Fishing nets and specific small-sized vessels are commonly found along the coastlines.

– Tourism: semi-enclosed seas are often popular tourist destinations due to beautiful beaches, favorable climatic conditions, and rich history. Regions around the Mediterranean Sea, for example, are renowned for tourist attractions. Typically, cities situated along the coastlines of such areas become tourist destinations. Recreational boating with small-sized vessels, speedboats, or sailboats is common in these regions.

– Energy exploration: in some semi-enclosed seas, there are energy resources such as oil and natural gas, which are exploited to meet global energy demand, leading to a predominant offshore industry. Coastal countries around these seas have developed this branch of the industry. Offshore platforms are commonly found in such areas. Additionally, pipelines on the seabed transport gases, petroleum products, etc. Recently, there has been an observed increase in the exploitation of renewable resources in these areas, such as the construction of wind farms.

Human activities hold considerable influence over the successful planning and execution of submarine operations, impacting a spectrum of aspects in this intricate domain. As I continue into the ensuing section of this article, I will be shedding light on the multifaceted ways in which human activities interlace with submarine operations.

1.3 Military Characteristics

Through the study of specialized literature, I have identified that semi-enclosed seas, from a military perspective, exhibit several crucial features for conducting underwater actions. In the paperwork "Influence of the Characteristics of the Black Sea on Joint Operations," authored by Dr. Florin Nistor and Dr. Ing. Lucian-Valeriu Scipanov, criteria for the analysis of semi-enclosed seas were presented, with the spatial and informational criteria being the most relevant for submarine operations among the four mentioned: "spatial, actional, temporal and informational."

Semi-enclosed seas are limited in space, and surrounded by land, thus reducing the operational area. The autonomy of platforms used in such areas will not be extensive, and military HVU (High Value Units) are positioned at relatively short distances (Nistor, Scipanov, 2021, p.27).

The paramount importance of submarines in a Black Sea conflict becomes readily apparent when one takes into account the military characteristics delineated by the authors mentioned earlier.

Examining how naval power manifests itself, through a careful analysis of notable military actions throughout history, it is observed that enclosed or semi-enclosed seas have been the predominant spaces for naval actions, especially in regional conflicts, and less so in major conflicts. (Milan Vego, 2013, p.11)

In conclusion, employing the three analytical characteristics has proven instrumental in discerning crucial aspects of semi-enclosed seas. These findings will, in turn, significantly contribute to realizing the objectives outlined in this article. Looking at the results and comparing them with other maritime areas such as open seas or oceans, it is acknowledged that the Black Sea would be a secondary theater of operations in the context of an extended conflict. However, the importance of controlling the sea is high in the initial phase of the conflict: “In the initial phase of the war in a closed sea, the main objective of a naval operation is to gain control of the sea” (Milan Vego, 2008, p.24).

II. Operating Submarines in Semi-Enclosed Seas - The Black Sea

Building upon the insights garnered in the preceding section, the objective is to delineate the operational characteristics specific to submarines operating in semi-enclosed seas, exemplified by the Black Sea.

The Romanian Naval Forces have a history of operating submarines, ranging from the so-called "pocket submarines" to conventional diesel-electric submarines. A brief history of Romanian submarines is presented by Cam. Fl. (rtr.) Dr. Ing. Constantin Rusu in the work "The Submarine” vol. 1. However, this history of the Romanian Naval Forces in the submarine domain was interrupted in 1996 due to the operational resource depletion of the Kilo-class submarine – "Delfinul".

The operational dynamics of submarines in the Black Sea are intricately tied to the unique characteristics of this region, presenting both challenges and opportunities that can be tactically leveraged in combat scenarios.

Based on the aforementioned physical-geographic attributes, I have identified distinctive operational features for submarines: navigation in shallow waters, execution of special maneuvers, continuous assessment of physical properties of water, and navigation in immersion in bottom currents.

Analyzing the depths of the Black Sea, especially those in the Responsibility Zone of the Naval Forces, it can be affirmed that these are waters with shallow depths. Therefore, the submarine's mode of operation must take this aspect into account. The possibility of detecting the submarine with aviation increases during submerged operations in such depths. Submarines will seek to operate in deeper waters. Regarding navigation in immersion where depths are shallow, submarine operations must consider the squat effect and the possibility of striking objects. Similarly, the submarine remains with limited maneuvering space. Taking the example of a Type 212 German submarine, it can navigate at periscope depth with a 12m water column under the keel but has limited vertical maneuvering space. Compact submarines are designed for operating in shallow depths. Thus, a constructive requirement can be identified for the opportunity to equip the Romanian Naval Forces with submarines – reduced constructive dimensions and the capability to operate in shallow waters. Submarines such as the Scorpene class, Type 212, 214, or S-18, etc., fall into this category.

In terms of the topography of the Black Sea's bottom, submarines can execute special maneuvers such as "bottoming" or stationing the submarine on the seabed. The topography of the Black Sea's bottom allows for the execution of such maneuvers. This action, where a submarine remains stationary on the seabed, significantly reduces the chances of its discovery by the enemy. During stationing, the submarine stops all systems on board, including ventilation, for two main reasons: one is that the systems are cooled with seawater, and by stopping them, the entry of objects from the seabed (sand, stones, etc.) through the hull penetrations is avoided, and the second is the total reduction of noise. This can only be performed by diesel-electric submarines since nuclear submarines cannot stop the reactor cooling.

Taking into account the physical characteristics of seawater, they bring about operational peculiarities. By the discharge of the Danube River into the Black Sea, a salinity difference is identified from north to south along the Romanian coastline. This can be used as an advantage for submarine operations but also as a disadvantage for the use of sonars and other sensors. Submarines can thus capitalize on the salinity difference that influences sound propagation in water. An essential requirement for submarines in such salinity difference conditions is the installation of continuous environmental analysis systems and sound propagation determination.

Marine currents also influence the submarine's mode of operation, especially navigation. In the Black Sea, a main current called the Circumbasin Current is identified, along with other smaller currents that move water masses in the opposite direction. Current movements can affect navigation in immersion. There is a need for equipping submarines with precise inertial navigation systems.

Regarding human activities in semi-enclosed seas like the Black Sea, they lead to submarine operational peculiarities, such as detailed planning of surfacing, operating in conditions with background noise, navigating in areas with intense fishing, and avoiding collisions with objects in immersion.

Naval traffic in the Black Sea within the responsibility zone of the Romanian Naval Forces is organized on recommended routes and has a higher density in port areas. It must be considered that intense traffic in semi-enclosed seas, especially in the Black Sea, can lead to accidents during surfacing or while navigating at periscope depth. Analyzing the traffic in the Black Sea reveals that the surfacing maneuver can be hazardous. Submarine surfacing actions must be well-planned and executed, as well as emergency diving maneuvers. In this regard, there is an example of a Japanese Naval Forces submarine that, during surfacing, collided with a commercial ship, causing material damage.

The density of commercial traffic and tourism with recreational activities leads to a high level of background noise for sonar operators. Thus, there is a need for operator training in noisy conditions and as an operational requirement – equipping submarines with sonars with noise filters.

For operating submarines in the coastal areas of Romania, fishing zones or areas must be taken into account. Getting entangled in fishing nets at the propeller can be a frequent problem. The energy exploitation in Romania's exclusive economic zone involves the existence of underwater structures such as oil platforms, gas or oil pipelines, and underwater cables. Such objects increase the risk of collisions in immersion. Equipping submarines with collision prevention and avoidance systems is another important requirement.

From a military perspective, other peculiarities in operating submarines in the Black Sea as a semi-enclosed sea are identified, such as battery management, maintaining secrecy, torpedo attacks from immersion, intelligence operations, and naval traffic monitoring missions.

As highlighted earlier, the Black Sea, as a semi-enclosed sea, is a confined space for conducting actions and presents short distances between military HVUs. As is known, the autonomy of conventional submarines (diesel-electric) is limited by the battery capacity. Thus, there is a need to develop a battery management system during submarine operations in immersion to extend the time for conducting combat and mission deployment. This should be a tactical and logistical objective. A good battery management system leads to better maintenance and extended lifespan.

To prolong the submerged operational duration, it is imperative to outfit submarines with air-independent propulsion (AIP) systems. These systems can generate electrical energy without necessitating surfacing or reaching periscope depth.

From an action standpoint, the importance of submarines is crucial. As operational peculiarities, maintaining the secrecy of the position in the context of confined space is identified. Thus, the development of procedures on how future platforms will "maintain discretion" in the Black Sea is crucial. The distinctive element of surprise inherent in submarine operations against the enemy substantiates the theory that naval conflicts in semi-enclosed seas unfold swiftly. Leveraging strike capabilities from submerged positions, utilizing torpedoes, and/or missiles from advanced platforms confer a significant tactical advantage.

The presence of a submarine in immersion not only leads to the allocation of forces by the enemy but also to the allocation of time required for its search. In this context, from a temporal perspective, a submarine can "gain" time for conducting other actions in the event of a conflict in the Black Sea.

From an informational standpoint, submarine-type platforms have one of their main missions as intelligence operations. Consequently, these platforms play a direct role in shaping the recognized maritime picture through their mode of operation. Monitoring naval traffic from the underwater environment or at periscope depth can provide valuable information to the Naval Forces or allies for conducting military actions.

By equipping submarines with COMINT (Communication Intelligence) and ELINT (Electronic Intelligence) sensors that can be deployed in the middle of the Black Sea, new capabilities for advanced research for the Romanian Naval Forces emerge. Operating submarines for information gathering represents another operational peculiarity.

The inclusion of submarine-type platforms in the Romanian Navy's assets can increase Romania's military importance in the region. Thus, by operating submarines in the depths of the Black Sea, Romanian Naval Forces can carry out complex actions for sea denial and control. A presence in immersion leads the enemy to allocate resources and time for the purpose of locating the submarine. The presence of submarines can complicate and disrupt enemy naval operations, as they must manage the underwater threat in addition to those on the surface. Submarines add tactical complexity, as opposing naval forces need to develop and implement specific tactics to detect, track, and counter submarines. The presence of submarines makes precise identification of their location difficult, imposing additional pressure on opposing forces in managing the underwater threat.

In conclusion, operating submarines in a semi-enclosed sea, such as the Black Sea, has several peculiarities and can pose a challenge. By identifying the link between the characteristics of the semi-enclosed sea and the specific mode of submarine operations in such areas, I have been able to highlight certain technical and constructive requirements for such platforms that the Romanian Naval Forces may find opportune to acquire. Consequently, these could include diesel-electric submarines, compact – of reduced dimensions, equipped with high-performance inertial navigation systems, collision avoidance systems with underwater objects, COMINT/ELINT information gathering systems, and advanced sonars with sound analysis systems. Additionally, for the proper operation of these platforms, I identified the need for a logistic battery management system to increase their lifespan. To extend the duration of operation in immersion, the submarine can be equipped with an AIP (Air Independent Propulsion) system.

Conclusions

In conclusion, based on the three analysis criteria, I have identified the significant characteristics of semi-enclosed seas. From a physical-geographical standpoint, utilizing the analysis and comparison of semi-enclosed seas with open seas and oceans, I identified relevant features for the operation of naval platforms in immersion. I concluded that semi-enclosed seas have a high density of human activities across various economic sectors: tourism, fishing, maritime transport, and the energy industry. Considering the military analysis results, I acknowledged that the Black Sea would be a secondary theater of operations in the context of an extended conflict. At the same time, the importance of submarine platforms cannot be neglected.

Therefore, submarine operations in the Black Sea are closely tied to the specific factors of a semi-enclosed sea. Understanding and managing these factors are essential for ensuring the efficiency and security of underwater operations in this region. Overall, analyzing the submarine operating mode in semi-enclosed seas, such as the Black Sea, reveals the complexity of operating these platforms within naval operations.

By identifying the connection between the characteristics of semi-enclosed seas and the specific mode of submarine operations in such areas, I have highlighted certain technical and constructive requirements for such platforms that the Romanian Naval Forces may find opportune to acquire.

Given the specificity of the area, an optimal profile for a submarine-type platform operated by the Romanian Navy in the Black Sea can be outlined. The proposal is for an attack diesel-electric submarine, compact in terms of constructive dimensions, equipped with guided torpedoes, high-performance sensors, and potentially equipped with an air-independent propulsion system. Such submarines are in operation by various NATO states bordering semi-enclosed seas. Examples include Sweden with the "Gotland" class submarine, Italy with the Type 212 submarine, and Turkey and Greece with Type 214 submarines. However, Turkey also operates smaller submarines such as the STM-500.

It is easy to appreciate that the presence of Romanian submarines in the Black Sea could play a crucial role in projecting power and combat capability, contributing to regional stability and reinforcing Romania's geopolitical position as an important pillar of power on the eastern flank of NATO.

BIBLIOGRAPHY:

1. Dr. Florin Nistor, dr. ing. Lucian-Valeriu Scipanov, *Influența caracteristicilor Mării Negre asupra operațiilor întrunite,* Impact Strategic Nr. 3, Universitatea Națională de Apărare Carol I, 2021;
2. Milan N. Vego, *Naval Strategy and Operations in Narow Seas*, US Naval War College, Newport, Rhode Island, Ed. Routledge, 2013;
3. Admiralty Sailing Directions: Black Sea and Sea of Azov Pilot (NP24), 6TH EDITION 2019;
4. Mikulsky Z., *Water balance of semi-enclosed seas,* Institute of Phisico-Geographic Science, Warsaw, Poland, 1976;
5. Terry Healy, Kenichi Harada, *Definition and physical characteristics of the world's enclosed coastal seas*, Marine Pollution Bulletin, Volume 23, 1991, Pag 639-644;
6. Milan N. Vego, *Major Naval Operations,* US Naval War College, Newport, Rhode Island, Ed. Routledge, 2008;
7. Milan N. Vego, *Submarines in Soviet ASW Doctrine and Tactics, Naval War College Review*: Vol. 36: No. 2, Article 1, 1983.
8. MXP-1(D) - Multi-National Submarine and Anti-Submarine Exercise Manual;
9. MTP-57 - The submarine search and rescue manual;
10. Cam. Fl. (rtr.) Dr. Ing. Constantin Rusu, *Submarinul vol. 1 - Evoluția submarinului (din cele mai vechi timpuri până în anul 2010)*, Editura Teophilius, București, 2019;
11. Damaschin Ioan, *Război submarin la Marea Neagră*, Editura Militară, Bucureşti, 2016;
12. Tangredi, Sam J. *The Good, the Bad, and the Stealthy: Surface Views of the Future of the Submarine Force (or A view from After Steering)*, Submarine Review, October 2001;
13. Clark, Bryan, *The future of the undersea deterrent: a global survey*, Australian National University, National Security College, 2015;
14. Stohs, Jeremy, *How High? The Future of European Naval Power and the High-End Challenge*, Centre for Military Studies, Copenhagen, 2021;

15. Milan N. Vego, *The Right Submarine for Lurking in the Littorals*, U.S. Naval Institute Proceedings, Vol. 136, Iunie 2010;
16. www.marinetraffic.com
17. https://english.kyodonews.net/news/
18. https://www.naval-technology.com/
19. https://www.janes.com/intelligence-resources/

1053477-3045-1396-24-24

CONSIDERATIONS ON THE EVOLUTION AND USEFULNESS OF HELICOPTERS IN MILITARY OPERATIONS

Cristian - Octavian STANCIU, PhD.
Colonel, Associate professor, PhD., "Carol I" National Defence University
Bucharest, Romania
E-mail: cristianstanciu73@yahoo.com

Cristian - Tiberiu CRISTESCU, PhD. candidate
Colonel, 2nd Mountain Brigade ,,Sarmizegetusa"
Brașov, Romania
E-mail: ccristi2577@yahoo.com

Abstract**:** *From basic to advanced, the doctrinal evolution, in conjunction with that of technology, paints a modern image for today's battlefield and the operational environment, both frequently transformable and continuously adaptable. The vertical axis component offers a different view of the battlespace, developing principles of combat that can be a game changer. Helicopters used in all types of military operations add value to army or naval forces in a binomial use.*

Keywords**:** *air support, air deployment, capability, evolution, air mobility, helicopters*

Introduction

The advent of helicopters in the immediate aftermath of the Second World War, and their subsequent development, further diversified the missions that aviation could perform for land, naval and special operations forces. Helicopters have, first and foremost, revolutionized troop mobility, removing all-natural obstacles to their mobility - hills and mountains, forests and swamps, terrain difficult for other means of transportation to reach.

Helicopters have changed the shape and structure of dismounted, maritime or air operations, created new possibilities for fire support to other forces, especially ground forces, created new possibilities for observation, search, discovery and surveillance of targets, CBRN recon possibilities, artillery fire control, etc. At the same time, the concept of *"vertical logistics"* has emerged, supplying isolated or independently acting forces, as well as providing medical evacuation from remote areas of conflict. Helicopters have also proved extremely useful in improving the troop command systems: *"In recent times, various command points have been set up on helicopters for certain echelons of land forces, thus achieving a more efficient, flexible, timely and, above all, continuous command. Such a command point can move quickly from one place to another."* (Major General Iosif Rus, Colonel Dr. Aureliu Cioabă, Vertical Component of Modern Warfare, Military Publishing House, Bucharest, 1988, p. 156)

Helicopters are an absolute necessity for naval forces as well. They have proven over the years to be particularly effective both in the fight against submarines and autonomous divers. Helicopters have also proven their effectiveness in combat actions carried out in cooperation with these types of assets (submarines or autonomous divers). For this reason, helicopter landing sites are established on almost all surface ships, while some others are even equipped deployable helicopters. In recent years, along aircraft carriers some naval forces have also begun deploying helicopter carriers. These developments are characterized as airborne operations, which in turn lead to the transformative character of strictly maritime operations, turning into aero-maritime or naval air deployment operations.

1. Helicopters and air mobility

The primitive iteration in which the helicopter, the *"autogiro"*, first appeared in the USA in 1923, attracted the attention of military leaders and it subsequently became a force multiplier that revolutionized the conduct of military operations in the mid-20th century. The use of helicopters by the US military has its origins in the Korean War, where they performed certain logistical support missions, particularly medical evacuation. The danger of a major war looming in Europe drew attention to the use of helicopters, both for transport and maneuver.

The maneuver elements available to the US Army at the time consisted of light infantry divisions, mechanized divisions and airborne paratroop divisions. These formations had different operational tasks and purposes, along with different combat capabilities. Thus, the light infantry had a slow movement speed and were supplied with difficulty, the mechanized units depended heavily on the accessibility of the terrain, even if they had a greater movement speed, while the paratroopers could be deployed anywhere in the opponent's depth, but once on the ground they turned into light infantry, with no resupply capabilities or fire support, apart from their own artillery and with a reduced maneuver capability.

The commander of an American army corps, General James Gavin, discovered from his war games in 1952 that his troops would suffer huge losses in the event of a tactical nuclear strike made by the Soviets. As a consequence, General Gavin put forward the idea of mass use of helicopters to disperse forces on the defense and concentrate them on the offensive. General Gavin's proposals, superimposed with the American experience in Korea and the intuition of other commanders of that time, led to the establishment of 12 transport helicopter squadrons in 1952, *"Although initially accepted only as an alternative means of transporting troops and supplies, the helicopter would later prove to be a radical innovative solution to battlefield maneuver." (Valerică CRUCERU, Insurgency, counterinsurgency and limited war, National Defense University Publishing House, Bucharest, 2005, p.169)*

1.1. Air mobility

After 1955, air mobility became an innovative concept developed by the US ground forces meant to replace mechanized combat, reconnaissance and transport assets with helicopters. Although the intentions of developing this concept were directed towards an eventual conventional warfare in Europe, the origin of its testing was in Vietnam, with the originators claiming that *"in difficult terrain, helicopters could be used with great success in reconnaissance and troop transport missions, for linkup, direct fire support and artillery maneuver, communications, supply and troop evacuation." (Valerică CRUCERU, Insurgency, counterinsurgency and limited war, National Defense University Publishing House, Bucharest, 2005, p.169)* Air mobility thus became an essential capability for the US military in the Vietnam War, especially for conducting counterinsurgency operations in South Vietnam. There were only two airmobile structures at the time: the *101st Airborne Division* and the *1st Cavalry Division*.

After the appointment of General Gavin as Chief of Land Forces Operations Directorate, efforts to implement air mobility in the Land Forces continued, and a new position of Aviation Chief was created. It is worth noting that the American experiences in Vietnam and the desire to create a new capability to ensure troop mobility laid the groundwork for the development of the concept of helicopter use by the ground forces. Following General Gavin's presentation to the decision-makers of the time of the helicopter use in army operations, a shift was proposed from ground marching columns to airborne ones, respecting the same scheme of the movement, with reconnaissance elements, security, maneuver, fire support and logistics. This would ensure a much greater mobility, offering the necessary conditions to adapt to the new combat environment. This gave rise to the idea of equipping all ground force units with helicopters, a mobility concept for the future. However, US policy makers did not approve such large sums of money to be allocated on such a project, especially with the reduction in defense spending for the army in favor of the air forces and the development of strategic airborne nuclear assets.

The concept of air mobility was once again promoted, 10 years later by General Hamilton Howze, who sought to convince the general staff of the army that air mobility kept the traditional tactical concepts viable, while adding additional value by increasing flexibility, even in the European landscape. General Howze organized a series of experiments at the Land Forces Command and Staff College between 1956 and 1958 to convince decision-makers of the need to develop the concept.

1.2 The helicopter in modern days

Recent events in Afghanistan, Iraq, the Ivory Coast and Libya bear witness to a double reality. While air mobility has established itself as a key asset in contemporary military operations, there is a parallel ongoing repositioning of the helicopter within the ground forces. Recent conflicts have provided a new relevance to the concept, *know-how*, developed 40 years ago, while on the other hand exposing the limitations of certain concepts inherited from the end of the Cold War, in particular attacks against formations of the enemy in the deep and also the envelopment maneuver at an operational level. These adjustments do not reflect the futility of these concepts as much as their inadequacy in the current context of engagement. In this process of reactive adaptation, it is necessary to review the most relevant changes that have occurred in the last 10 years.

It would be foolhardy to draw any definitive conclusions from the operations in Iraq or Afghanistan. However, given their specific character and duration, it is undeniable that these two conflicts have led Western forces to question the relevance of certain courses of action that have proved ill-suited for the circumstances. The helicopter has not escaped criticism and evaluation, as illustrated by the lessons identified and learned, a process initiated by the US armed forces from military actions in the two theatres of operations.

From the very first phase of Operation *Iraqi Freedom*, US and British ground forces identified air mobility as one of the factors contributing to the success of a blitzkrieg campaign, thus achieving a high rate of progression towards Baghdad. Helicopter-supported deep strikes conducted under the *Air Land Battle* doctrine, soon showed their limitations. Thus, on 23 March 2003, the *11th Attack Helicopter Regiment* flew a deep strike attack force mission involving two helicopter battalions to destroy the *Iraqi Republican Guard*'s *Medina Division*. The operation was a complete failure:" one *helicopter reached the target area, but had to fall back under heavy fire; of the 30 AH-64 Apaches involved in the operation, one was shot down and the other 29 heavily damaged*" (Anthony H. Cordesman, "The Strengths and Weaknesses of the A-64 Apache and other attack helicopters", The Iraq War, Strategy, Tactics and Military Lessons, CSIS, Washington, 2003, pp. 317-332). This failure was no doubt primarily caused by inadequate preparation and planning, whether intelligence, close air support, or lack of coordination due to the high tempo of operations. This failure was also caused because of the great efforts made by the Iraqi armed forces, who, unlike in the first Gulf war, understood the advantage gained by having a greater depth to their defense.

Based on the above-mentioned facts, it must be acknowledged the fact that the attack that took place on the 23rd of March did not cause any *"operational shock"* to the Iraqi command, failing from the outset as a battlefield shaping operation. On the contrary, it was a genuine shock to the US Air Force, challenging its traditional SOPs. On the basis of a single example, it is clearly difficult to know whether this fiasco was due to a fundamental conceptual error or whether it was the case of an error in execution. The Air Force, in agreement with the high command, no longer carried out attack missions of that type during the Operation *Iraqi Freedom,* concentrating instead on direct fire support to ground troops and gradually resurrecting courses of action abandoned at the beginning of the Vietnam War.

For example, the 101st Airborne Division was involved in heavy fighting near Al Hillah against a Republican Guard battalion, using the full range of common assets (tanks, artillery battery, air defense systems). In close cooperation with the ground forces, 101st Airborne Division helicopters provided fire support to ground units using the so-called Close Combat Attack (CCA) or Close Combat Support (CCS) procedure. Eight AH-64 Apache helicopters were hit by the enemy, but all remained operational without being shot down due to their high level of protection. Ultimately, the AH-64 Apache performed a wide range of combat and reconnaissance missions, during day and night, helping to destroy important targets such as artillery and air defense batteries. This type of operation depended on close coordination with the ground forces, as well as with the A10's Close Air Support (CAS) or reconnaissance aviation. Identified at ranges of up to eight kilometers, targets were engaged using all available resources.

In Afghanistan and Iraq, the danger coming from light infantry weapons, assault rifles and anti-tank rocket launchers, sometimes associated with air defense weapons was highlighted. More than the weapons themselves, the real threat came from their dispersal and their tactically relevant use in terrain whose characteristics were unfavorable to helicopters, such as high mountains or urban areas. Not only were traditional detection and combat systems inoperative, but low-altitude flight could be very dangerous in some cases, as it was well illustrated on the 23rd of March 2003 attack, an attack during which the helicopter crew was saved only because of the protection provided by the aircraft. Attack helicopters continued however to perform combat and support missions. In terms of combat in urban areas, for example, the 101st Airborne Division showed its adaptability, using tactics that proved their effectiveness. The cavalry's Kiowa helicopters were used directly in built-up areas for scouting and surveillance. Faster and more maneuverable, these helicopters were harder to hit than the AH-64 Apache, which remained in combat support positions close to urban areas, to be used in larger-scale attacks. The Americans used this type of tactic in the densely vegetated Afghan valleys in mutual support of ground forces using the previously mentioned Close Combat Attack (CCA) procedure.

In stability and support operations, as well as in counter-insurgency actions, the helicopter has had and will have a key role, making it possible to operate in an entire theatre of operations, with forces that are smaller in size. In 2004, the US military had more than 500 helicopters deployed in Afghanistan and Iraq.

Not only has the helicopter substantially reduced response time due to its speed, but it has allowed forces to bypass terrain barriers and evade the omnipresent threat of IEDs (improvised explosive devices) when facing insurgents who are disguised among the local population.

In other words, the operational and tactical mobility of the helicopter illustrated and confirmed the three basic principles of war according to Foch: preserving freedom of action, concentrating efforts at a given time and place, and speed of action, which are very well complemented by the fourth principle of combat: surprising the adversary while trying to avoid being surprised in turn. Finally, the helicopter also played a key role in terms of logistical support and medical evacuation. From a psychological point of view, this last point is fundamental, as it means that the soldier is virtually guaranteed a quick and safe evacuation. The French helicopter battalion deployed in Kabul was involved in 160 medevac missions in 2010, with an average of 1 hour 30 min between the alert call and the arrival of the casualty at the military base. Finally, it is important to note the primary role of helicopters in covering the three basic combat functions: maneuver, fire support and logistic support. Clearly it is easy to demonstrate that helicopters are an extremely important capability for ground forces, with major influences on the other combat functions as well. The CH-47 Chinook has established itself as the transport helicopter of US and British forces due to its rugged design, logistical and tactical transport capabilities. The ability to load a platoon or company in a single helicopter along with a few vehicles, make the CH-47 Chinook a valuable tactical asset and a solid security guarantee. Similarly, in Iraq and Afghanistan, as in other theatres of operations, special operations have played and continue to play a decisive role. As Operation Geronimo, which led to the elimination of Bin Laden, recently demonstrated, the helicopter is the preferred means of infiltration for such units, due to its unique capabilities.

Profound changes in the role of helicopters raise important questions about the organization of command and control structures. While France and the US have traditionally developed helicopter forces with a strong ground orientation (operational ground attacks without relying on ground-level movements), other models exist. The increased altitude at which helicopters operate, their weaponry, tempo and types of roles they can fulfill pose a series of problems when it comes to deconflicting and coordinating air operations.

In Israel, helicopters are placed under the full authority of the Air Force. Used in direct support of ground maneuvers, helicopters served as a genuine link between the army and air force, which suffered from a dramatic lack of coordination during the Yom Kippur War. Helicopters were also involved in detecting and destroying portable and light defensive systems that posed a high risk for aviation assets. AH-1 *Cobras* and AH-64 *Apaches* conducted reconnaissance flights in order to gather intelligence and disseminate it to the proper stakeholders.

During the 2nd phase of the Lebanon operation, the need for a better coordination at the joint level was already obvious. During certain phases of the operation, attack helicopters were transferred under the direct command of the Ground Forces to address this problem. Ultimately, problems arose in the relationship between the engagement of targets and airspace management due to restricted space and lack of coordination between fixed-wing aircraft, helicopters, UAS and artillery. This lesson seems to have been learned during Operation Cast Lead in Gaza and has now led to a functional strategy using helicopters under direct air force coordination.

In the UK, the distribution of helicopters in accordance with the battlespace needs is organized according to machine type and functionality between the Royal Air Force for transport helicopters and the British Land Forces for reconnaissance and attack helicopters. This has created the need for a joint force to coordinate operations. Initially developed to rationalize maintenance costs, the requirement for better coordination led to the establishment in 1999 of the Joint Helicopter Command (JHC), a unified command structure that considers the specific differences of each category of forces. The JHC has the authority to operate all attack helicopters except those involved in rescue missions and those deployed on frigates.

This traditional organization posed problems during the deployment of British troops to Iraq during Operation Telic. The way helicopters were deployed led to redundant chains of command and unsatisfactory allocation of aircraft to the ground units. The reconnaissance and attack helicopters of the army were subordinate to the 16 Air Assault Brigade, while the utility helicopters of the Royal Air Force and the Naval Forces were grouped under a single command structure. Other units had no dedicated structures at all. The British Army responded to this situation by creating a joint command structure, the Joint Helicopter Force Iraq, responsible for all resources dedicated to air-to-ground combat. However, the units still remained separated and each branch continued to allocate specific aircraft types. This command structure was also adopted during Operation Herrick in Afghanistan.

In this respect, the British Army's vision differs from the organization of the US and France, which prefer to integrate all air-to-ground combat air assets into their land forces.

In France, where the army has a historical supremacy over rotor aircraft, progress towards a coordinated and a unified battlespace has been gradual and dictated by the arising needs. The Joint Helicopter Command (Commandment Interarmees des Helicopteres, CIH) was created in 2009 under the command and authority of the Chief of the Land Forces Staff (CEMA); with the task of optimizing, coordinating and harmonizing the missions of the army with the helicopter aviation component. As in other environments, crews were influenced by the organizational culture of their own branch and maintained specific characteristics designed to complement the operational tasks of the army. Increased coordination required the establishment of helicopter standards, with a focus on standardization of training and qualification.

The initiative seems to have been successful because at the end of 2009, the helicopter battalion in Kabul (Bathelico) were able to aid the French troops in Afghanistan with elements from different branches under its command (12 aircraft, including one from the Air Force). In any case, no one should believe, under any circumstance, the work that needs to be done in order to achieve a joint spectrum; contrary to the British equivalent, the CIH has no authority to use the aircraft, but instead acts as an indirect guidance tool through CEMA. Far from beating the end goal, this initiative is the first step towards building a close link in a process where the biggest challenge is to increase interoperability between the military branches without losing the specific knowledge of each.

Helicopters will be subjected to numerous trials during the coming years, judging by their various capabilities, industry and tactical-operational requirements that have been identified in recent operations. Certainly, the entire mission spectrum is now fully covered - from logistics and medical evacuation, to deep strikes, fire support and mobility - signifying a peak in the technological cycle. Going forward, however, the ultimate task will be to find acceptable terms of engagement in the face of a widening gap between the doctrine and strategic ambitions of the armed forces on one hand and the economic and budgetary realities of a system whose costs are now open-ended, on the other.

Considering the recent lessons learned and foreseeable trends, the need for air mobility operations should in all likelihood be confirmed in the near future. However, the technological orientation of Western nations seems to be reaching certain limits through a combination of increasing cost effects and budgetary difficulties. In these circumstances, the armed forces are opting for a mix of structures with an integration of different weapons systems, which were designed from the outset to be adaptable and modular, in order to improve their effectiveness and control the costs. This reality also applies to helicopters: armies adapt their current aircraft platforms in order to try and anticipate the future need of such platforms. While many innovations such as UAVs are as promising as can be, there are other scenarios that could pose a problem for rotary aircraft.

Over the last decade the average cost of military equipment has gradually increased. Aircraft have made no exception to this rule, and in particular the emergence of the new generations of helicopters. This increase is partly influenced by technical and technological development, but there are other causes as well.

Firstly, it is necessary to consider the exact the nature and specifications related to the development of military helicopters. When a commercial operator wishes to purchase a civilian helicopter, the first consideration is the payback period. The helicopter is often intended to fulfil a specific role, with an intense use in a short period of time, generally with little involvement coming from other machinery. In the military environment the approach is totally different. In general, procurement covers a whole fleet of helicopters, which must be intended as a response to a wide range of missions undertaken in the most advantageous conditions (day and night, temperature and weather). Combat helicopters must withstand damage coming from a wide area of projectiles, which means a duplication of vital systems, use of complex materials and increased structural weight, which is a serious handicap in aeronautical terms. Helicopters must achieve a high performance in terms of engine, noise reduction, range, etc. The weapon systems must integrate the capability of data acquisition, communications and target systems, together with a whole range of fire suppression systems, the use of which generates significant structural problems. These machines have a life cycle of at least 20 years, which in practice can double, and the rate of use can vary according to circumstances. Finally, as with any aircraft, precautions must be taken to avoid equipment failure, which is usually fatal. Considering this list of requirements, it becomes easy to understand the difficulties the military environment has in estimating costs and the difficulties the industry has in maintaining them. These difficulties can increase considerably when it comes to designing a new helicopter prototype.

Secondly, a mention should be made about the key importance of air defense considerations. Underpinning the issues of national defense, one of the core competences of any state, weapons programmed with a high development and production costs have nowadays led to partnerships between several countries. Aeronautics is an area in which excellence is achieved through science and designed with dual application in mind. Companies possessing this type of knowledge are relatively few in number, but compete in a highly competitive market. By agreement, each state, even in a tight budgetary period, must monitor the long-term status of this industry. Under these circumstances, politics, security, finance, industry and economic issues are closely related. The increase in the cost of a specific equipment must be analyzed through the lens of such issues.

In reality, development and production through the means of an international cooperation means that the difficulties inherent in running that programmed are increased in scale and complexity. As an example, there is sometimes an excessive amount of time when it comes to negotiations between partners who sometimes are hesitant and delay the research/production. As an illustration of this is the first Franco-German discussion on the *Tiger* helicopter which took place in 1975, but the development contract was not signed until 1992, 14 years later. The same observation can be made about the NH90, whose development was not completed until 1992, even though it was scheduled to enter service in 1990. Furthermore, a major drawback of cooperation, while by definition the requirement of the platform is to reduce the costs of production, the modifications and special features required by a particular country in terms of system specifications end up transforming the concept of "ready-made" into a "custom-made" machine. The NH90 currently comprises more than 20 different variants.

Finally, reducing the number of units ordered, for whatever reason (budgetary constraints, changes in the operational context), automatically leads to an increase in the cost per unit. In broad terms, this increase has an impact on the budget and completes a vicious circle causing a further reduction in units ordered. There are only a few companies that can regularly withstand significant changes in design specifications. France's requirement for the *Tiger* helicopter was reduced from 215 units to 80 resulting in a 78.1% cost increase (Court of Auditors, Rapport public annual 2010, February 2010, p.51, accessible at: http: www.ccomptes.fr/fr/CC/Sommaire-23.html.). The same phenomenon can be observed in the case of the NH90, where the reduction from 220 to 160 units resulted in a cost increase of 21.4% (Court of Auditors, Rapport public annual 2010, February 2010, p.51, accessible at: http: www.ccomptes.fr/fr/CC/Sommaire-23.html.). Delays in production have also other major sources of cost increases, from technical or industrial difficulties, the extension of orders for budgetary reasons to a combination of the factors mentioned above.

Taking all this into account, it is easy to understand that what is presented at first glance is a massive increase in the cost of conversion from one generation of helicopters to another (between Gazelle and Tiger the percentage was 1 to 25). The increases in acquisition and maintenance costs inevitably have an influence on how these platforms are used and reinforces a cautious trend in dealing with such acquisitions in the future. It also influences future trends in military structures, or in terms of aircraft, the number of platforms required, available or ultimately a mix that is destined to become a long-term feature of helicopters in the West.

Conclusions

After their rather humble beginnings, helicopters were at one time seen as the future of ground combat, the new combat weapon replacing the battle tank, both tactically and grouped in division-level formations and beyond, operating behind enemy lines. This vision, typical for the end of the Cold War, has proved poorly adapted to the political conditions and operational realities of today's conflicts, where Western armies are more sluggish because of their forces being dispersed on campaigns combining stability and support, while in some cases counter-insurgency operations. Western air forces have had to adapt and rediscover some tactics and procedures used 40 years ago when the helicopter was making its debut as a combat platform. They have been very successful in this effort, combining various types of operations conducted by the latest generation of platforms incorporating the latest technological advances as well as integrating, on a lesser extent, the support provided by older types of helicopters.

Valid for both attack and utility helicopters, this distribution of roles is intended to complement one another and promote the idea of maintaining mixed fleets combining several types and generations of aircraft. This is the only way for the air force to meet the many demands that present themselves in the coming future.

Faced with a broad spectrum of missions in theatres of operations that are often vast and harsh, demands for tactical transport and systems that can provide decisive coverage and engagement of the target will remain high and perhaps even increase.

However, many questions remain unanswered, particularly in terms of costs. As long as there is no doubt regarding the need for helicopters, the ability of European forces to meet this need remains highly problematic. Combined with the continuing decline in defense spending, which seems most likely to continue under the impact of the current economy and budget crisis, the procurement and ownership costs of the latest generation of platforms are a burden on the budget of the French army which has already been forced twice to reduce the number of aircraft originally planned. In order to guarantee the medium-term viability of the military forces nowadays, it is therefore essential to achieve a much better cost control ratio. Some elements of the response to this issue already exist, starting with the intent of outsourcing certain functions, continuing with the idea of mixed aircraft fleets that are tailored and optimized with an undefined mix of advancement and modernization, while also involving some delicate trade-offs in the defense budget and between different services and agencies.

Today's helicopter is a potential autonomous system, a permanent support solution and modern cavalry for the army, as well as the true workhorse for all services, with multiple roles combined into one. It constitutes an indispensable capability, in direct link with a strong demand for such capabilities. The same idea is going to apply in the future as well, with extra benefits for countries that are able not only to integrate their air assets into ground maneuvers, but also to take full advantage of the possibilities offered by digitization and real-time control of the engagement area with the use of strike aircraft and in cooperation with UAVs or by conducting true joint air operations.

BIBLIOGRAPHY:

1. Major General Iosif Rus, Colonel Dr. Aureliu Cioabă, Vertical Component of Modern Warfare, Military Publishing House, Bucharest, 1988
2. Valerică Cruceru, Insurgency, counterinsurgency and limited war, National Defence University Publishing House, Bucharest, 2005

3. Anthony H. Cordesman, "The Strengths and Weaknesses of the A-64 Apache and other attack helicopters", *The Iraq War, Strategy, Tactics and Military Lessons,* CSIS, Washington, 2003
4. Court of Auditors, Rapport public annual 2010, February 2010, p. 51, accessible at: http: www.ccomptes.fr/fr/CC/Sommaire-23.html.
5. Deodat du Puy-Montbrun, L'Honneur de la Guerre, Paris, Albin Michel, 2008
6. Rodney R. Propst, The Marine Helicopter and the Korean War", Combat Studies Center, 1989
7. John J. McGrath, Fire for Effect: Field Artillery and Close Air Support in the U.S. Army, Fort Leavenworth, KA, U.S. Army, Combat Arms Center, Combat Studies Institute Press, 2008.
8. James Gavin, "Cavalry and I Don't Mean Horses", Harper's, April 1954.

1053477-3045-1396-24-25

RESEARCH AND DEVELOPMENT TRENDS IN TACTICAL COMMUNICATION FOR MILITARY APPLICATIONS

Alina-Florentina PLĂPĂMARU
Eng., research assistant, Military Equipment and Technologies Research Agency,
Bucharest, Romania
E-mail: aplapamaru@acttm.ro

Denisa PETRAȘCU
Eng., research assistant, Military Equipment and Technologies Research Agency,
Bucharest, Romania
E-mail: dpetrascu@acttm.ro

Abstract: *Tactical communications play a crucial role in military operations, serving as the backbone for coordination, command, and control on the battlefield. Effective communication is essential for ensuring the success and safety of military units. The field of research and development (R&D) in tactical military communications is dynamic and continually evolving, including major topics like: AI for optimizing communication networks, automating decision-making processes, and enhancing cognitive communication capabilities, mesh networking for decentralized communication, cognitive radio systems. The integration of unmanned systems and Internet of Things (IoT) devices into military communication networks was increasing. This trend aimed to improve situational awareness and enable more effective coordination between human-operated and autonomous systems.*

Keywords: *Command and Control, TACCOM, Real-time Information Exchange, Electronic Warfare, Situational Awareness, radio systems, 5G, AI*

Introduction

Tactical Operations are becoming very complex, necessitating advanced communication platforms and Interoperable Communication Server to manage both battlefields and law enforcement missions.

The Tactical Communication Systems consist of an Integrated Communication System (ICS) which works as an Interoperable Communication Server. ICS ensures a reliable, jam-resistant and encrypted information exchange among forces, even if they are operating on different radio frequencies or different kinds of radios.

"Tactical Communication Systems are used within or in direct support of the operational forces and are designed to provide a secure, Integrated Communication System and an Interoperable Communication Server for voice, data, and video, among the various forces involved to facilitate command and control of the operation.

Tactical communication systems, an integral part of tactical operations centers (TOC) act as command and control posts for police, paramilitary, or military operations that provide a fully Integrated Communication System enabling trained officers and military personnel who guide the active team during a mission." (Solutions 2020)

"The role of the tactical communication systems is to be able to support the force regardless of the nature of its deployment. In the extreme, the tactical communications system must be able to provide communications in conventional high-density deployments where brigades might be deployed with a 25-km frontage, as well as support widely dispersed deployments to support modern operations in which a single brigade-sized force may have frontages of several hundreds of kilometers." (Ryan 2011, 5)

The evolution of tactical communication systems has been marked by a dynamic trajectory, driven by advancements in technology and the evolving nature of modern warfare. Over the years, these systems have undergone significant transformations to meet the increasing demands of complex operational environments.

"For the first several millennia, military communication took one of two simple forms: signaling by some visual or acoustic means, or the relaying of a message by runner or courier.

- 1873 – invention of the Morse Code
- 1853 – the telegraph was employed for the first time in war during the Crimean War
- 1859 – the electrical telegraph was used by the Spanish during the war with Morocco
- 1886 – US Army was using the telephony for the first time during the Geronimo campaign in Arizona
- 1898 – Marconi had developed his radio to the point that he managed to span the English Channel
- 1903 – a suitable wireless telegraphy was developed for Army use
- 1918 – first voice radio sets (radiotelephone sets) were introduced
- 1934 – the US developed the first walkie-talkie (the 25-pound radio)
- 1943 – the frequency modulation (FM) radio was developed to provide noise-free communications" (Ryan 2011, 5)

Figure no. 1. SCR 284 Radio System (US Army)

The modern history continues with:

1940s - Radios and Signal Corps: During World War II, radios became crucial for military communication, enabling commanders to coordinate troops over long distances. Post-war, advancements in portable and reliable radios continued, enhancing mobility and flexibility on the battlefield. The Signal Corps played a vital role in operating and maintaining these communication systems.

1940s-1950s - Encryption and Secure Communication: The importance of secure communication was recognized during World War II, leading to the development of encryption techniques. This continued post-war with the adoption of encryption technologies like cipher machines. Efforts to secure military communications intensified with the development of digital encryption methods.

1950s-1960s - Microwave Communication: Advancements in microwave technology post-World War II facilitated the development of microwave communication systems for military use. These systems allowed high-speed transmission of voice, data, and video over long distances, improving the efficiency of military communication networks.

1960s-1970s - Satellite Communication: Artificial satellites emerged in the late 1950s and early 1960s, revolutionizing military communication by providing global coverage and connectivity. Military satellite communication systems offered secure and reliable links between distant locations, reducing reliance on ground-based infrastructure.

1980s-1990s - Digitalization and Networking: With the rise of digital technologies, military communication systems transitioned from analog to digital, enabling faster transmission and better signal quality. Network-centric warfare concepts emerged, emphasizing the integration of various communication systems for a unified battlefield environment.

1990s-2000s - Mobile Communication and Command Systems: Mobile communication systems and command-and-control (C2) platforms gained prominence, allowing commanders to maintain situational awareness and coordinate operations in real-time. Tactical radios and mobile command centers became essential components of modern military forces.

2000s-Present - Cybersecurity and Information Warfare: As military communication systems became increasingly reliant on digital technologies, cybersecurity and information warfare emerged as significant concerns. Efforts to enhance cybersecurity measures and develop capabilities for offensive and defensive cyber operations became crucial in modern military communication strategy.

Figure no. 2. Falcon IV Family Radios (L3Harris)

Tactical communication plays an important role in supporting military operations by providing real-time communication and intelligence data.

"Tactical communication enables military personnel to establish reliable and secure communication links in remote areas, where traditional infrastructure may be absent or unreliable. This ensures that troops stationed in remote regions can communicate effectively, resulting in improved coordination and operational efficiency." (One 2023)

Tactical communication plays a very important role in military operations because it enables information sharing, safe communication, effective coordination, situational awareness, real-time information exchange and logistical support. Also, tactical communication allows military units to adapt very quickly to changing circumstances.

Tactical communication plays a crucial role in military operations for several reasons, such as the following:

Coordination and Command: Tactical communication allows commanders to coordinate movements, issue orders, and direct troops in real-time. Effective communication ensures that units are synchronized and can respond promptly to changing situations on the battlefield.

Situational Awareness: Clear and timely communication provides soldiers with vital information about the battlefield environment, including enemy positions, terrain features, and friendly unit locations. This situational awareness is essential for making informed decisions and adapting to evolving threats.

Fire Support and Close Air Support: Tactical communication enables the coordination of fire support assets, including artillery, mortar units, and close air support aircraft. Clear communication between ground forces and supporting elements ensures accurate targeting and minimizes the risk of friendly fire incidents.

Logistics and Resupply: Effective communication is essential for coordinating logistics and resupply operations. Units must communicate their needs for ammunition, fuel, medical supplies, and other essential resources to ensure they remain operational and capable of sustaining combat operations.

Reconnaissance and Intelligence: Tactical communication facilitates the exchange of reconnaissance and intelligence information between units, allowing for the rapid dissemination of critical intelligence updates and situational reports. This information sharing enhances overall situational awareness and helps identify enemy vulnerabilities.

Force Protection: Communication is vital for implementing force protection measures and responding to threats effectively. Units must be able to communicate warnings, requests for assistance, and emergency situations to ensure the safety and security of personnel.

Flexibility and Adaptability: Tactical communication systems must be flexible and adaptable to support the dynamic nature of military operations. They should allow for rapid reconfiguration and interoperability between different units and command levels to meet changing mission requirements.

Security and Encryption: In modern warfare, ensuring the security of communication is paramount. Tactical communication systems employ encryption and secure protocols to protect sensitive information from interception and exploitation by enemy forces.

1. Current state of tactical communication systems for military applications

In recent years, tactical communication systems have made a transition from analog to digital formats.

"In the wake of speedy technological advancements, command-control communications, computers, information and intelligence, surveillance and reconnaissance (C4I2SR) systems provide sterling opportunities to the defence and security establishment, acting as important force multiplier for commanders at all levels.

Continuously evolving solutions for battlefield communications have come a long way over the years, to the highly-advanced networks operating today. With secure communications being crucial for military operations, commercial and government entities are continuously working to improve available solutions.” (Forces 2019)

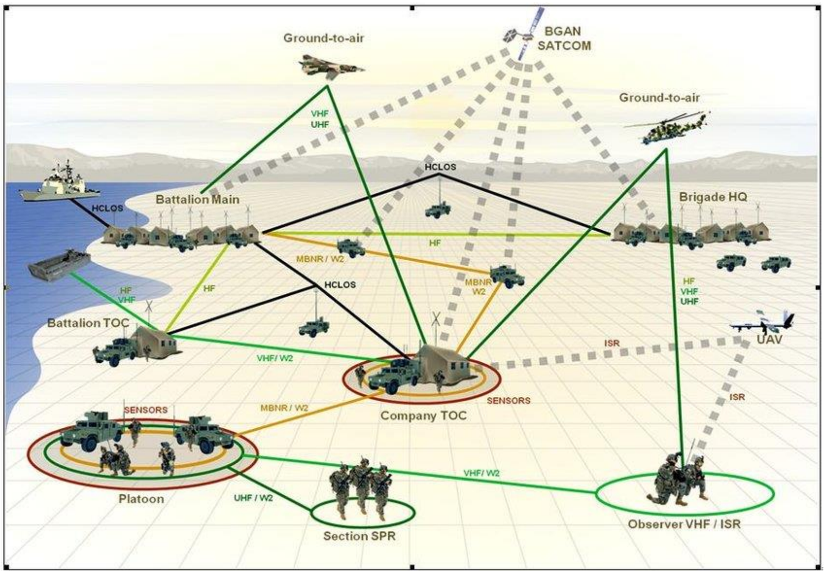


Figure no. 3. Harris-Integrated-Battlefield-Communications-Network Architecture

Recent advancements in military tactical communication have propelled the field to new heights, leveraging cutting-edge technologies such as:

1. *Software-Defined Radios (SDR):* SDR technology allows for greater flexibility and interoperability in military communication systems. It enables rapid reconfiguration of radio frequencies, waveforms, and protocols, making it easier for different units and platforms to communicate seamlessly.
2. *Integrated Networked Communication Systems*: Modern military communication systems are increasingly integrated into networked architectures, allowing for the seamless exchange of voice, data, and video across diverse platforms and domains. This integration enhances situational awareness and decision-making capabilities on the battlefield.
3. *Satellite Communication (SATCOM) Enhancement*: Advances in satellite communication technology continue to improve the bandwidth, reliability, and resilience of military SATCOM systems. High-throughput satellites, advanced ground terminals, and anti-jamming capabilities enhance the ability of military forces to communicate securely over long distances and in challenging environments.
4. *Advanced Encryption and Cybersecurity*: With the growing threat of cyberattacks and information warfare, there is a heightened focus on advanced encryption techniques and cybersecurity measures to protect military communication systems from exploitation and disruption. Quantum-resistant encryption, secure key management, and intrusion detection systems are among the latest developments in this area.
5. *Cognitive Radio and Spectrum Management:* Cognitive radio technology enables dynamic spectrum access and intelligent spectrum management, allowing military communication systems to adapt to changing electromagnetic environments and avoid interference. This capability enhances the reliability and effectiveness of communication networks in congested or contested spectrum environments.

Figure no. 4. Radio cognitive systems principle

6. *Unmanned Systems Communication Integration*: Integration of communication systems into unmanned platforms, including drones, autonomous vehicles, and unmanned maritime vessels, enables enhanced situational awareness and remote operation capabilities for military forces. This integration allows unmanned systems to communicate with manned platforms and command centers, facilitating coordinated operations.
7. *Artificial Intelligence (AI) and Machine Learning (ML):* AI and ML technologies are increasingly being applied to optimize military communication systems, including adaptive waveform selection, predictive maintenance, and network optimization. These technologies improve the efficiency, reliability, and resilience of communication networks in complex and dynamic operational environments.
8. *Secure Mobile Communication Solutions*: Mobile communication solutions tailored for military use, including ruggedized smartphones, tablets, and tactical apps, provide soldiers with enhanced connectivity and situational awareness on the battlefield. These solutions incorporate advanced security features such as end-to-end encryption and secure messaging to protect sensitive information.

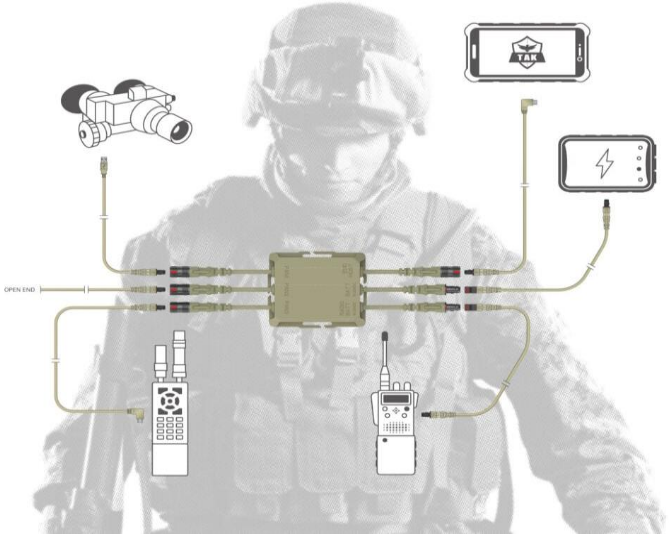


Figure no. 5. Digital combat soldier

2. Future prospects and predictions

The field of TACCOM (tactical communications) is a field in continuous development which brings important transformative changes in military operations, changes driven by rapid advancements in technology and evolving operational requirements.

“The future of the global tactical communication market looks promising with opportunities in the command & control, intelligence, surveillance & reconnaissance (ISR), situational awareness, and routine operations markets.” (Lucintel 2024)

In envisioning the future of military tactical communication, a convergence of cutting-edge technologies and strategic imperatives promises to reshape the landscape of battlefield connectivity.

From the advent of 5G networks and artificial intelligence-driven systems to the prospect of quantum communication and biologically-inspired solutions, a host of transformative advancements stand poised to revolutionize how military forces communicate, coordinate, and operate in the theater of modern warfare. With the integration of space-based assets, cyber-physical synergies, and biometric sensing capabilities, the horizon of military communication holds unprecedented potential for enhancing command effectiveness, situational awareness, and operational resilience in an increasingly complex and contested environment.

1. *5G and Beyond*: The deployment of 5G networks will revolutionize military communication by providing ultra-fast, low-latency connectivity for troops in the field. Beyond 5G, emerging technologies such as 6G and terahertz communication hold the potential to further enhance data transmission speeds and network reliability, enabling new capabilities for military operations.
2. *AI-Driven Communication Systems*: Artificial intelligence and machine learning will play an increasingly significant role in optimizing military communication systems. AI-powered algorithms will automate spectrum management, adaptive waveform selection, and network optimization, allowing for more efficient use of resources and improved resilience in dynamic operational environments.
3. *Quantum Communication*: Quantum communication holds the promise of unbreakable encryption and secure communication channels immune to eavesdropping or interception. Research in quantum key distribution (QKD) and quantum teleportation could lead to the development of ultra-secure communication networks for military use, protecting sensitive information from cyber threats and electronic warfare.
4. *Swarm Communication*: The proliferation of unmanned systems and autonomous platforms will drive the development of swarm communication technologies. Swarms of drones, robots, and other autonomous assets will communicate and collaborate seamlessly, enabling coordinated actions and distributed intelligence gathering capabilities for military forces.

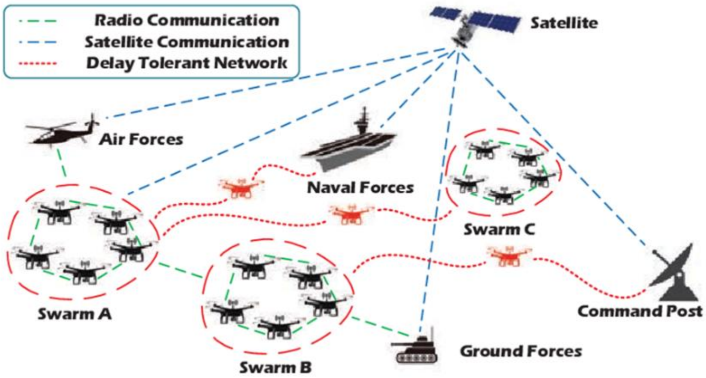


Figure no. 6. A model of swarm UAVs in battlefield

5. *Biologically-Inspired Communication*: Bio-inspired communication systems, inspired by the collective behaviors of social insects and animals, could offer novel solutions for resilient and adaptive military communication networks. Concepts such as self-organizing networks, swarm intelligence, and adaptive routing algorithms may be applied to enhance communication reliability and survivability in contested environments.
6. *Space-Based Communication*: The growing militarization of space will lead to increased reliance on space-based communication systems for military operations. Next-generation satellite constellations, including low Earth orbit (LEO) megaconstellations and high-throughput satellites, will provide global coverage and high-bandwidth connectivity for troops deployed anywhere on the globe.
7. *Cyber-Physical Integration*: The integration of cyber and physical domains will blur the lines between traditional communication networks and cyberspace. Military communication systems will be tightly integrated with cyber operations, employing techniques such as cognitive electronic warfare and network-centric cyber defense to protect against cyber threats and maintain operational superiority.
8. *Biometric Communication*: Advancements in biometric sensing technologies will enable new forms of communication based on physiological signals such as brain waves, heart rate, and facial expressions. Biometric communication systems could offer secure and covert communication channels for military personnel, enhancing operational security and situational awareness on the battlefield.

Conclusions

The field of tactical communications is in continuous development, improving interoperability, strengthening cybersecurity, coordination and operational efficiency.

Tactical communication systems enable more effective and efficient military operations and these systems will continue to evolve to meet the needs and challenges of modern warfare.

The advancements in tactical communications field are pivotal in enhancing the practicality of military applications. The emerging technologies presents real challenges to military communications in tactical situations.

In conclusion, the evolution of military tactical communication is poised for remarkable advancements driven by cutting-edge technologies and emerging strategic imperatives. As we look ahead, the convergence of 5G networks, artificial intelligence, quantum communication, and biologically-inspired solutions promises to redefine how military forces communicate, collaborate, and confront challenges on the modern battlefield.

These transformative developments hold the potential to enhance command effectiveness, improve situational awareness, and bolster operational resilience in the face of evolving threats. By integrating space-based assets, leveraging cyber-physical synergies, and harnessing biometric sensing capabilities, military communication stands at the cusp of unprecedented innovation, offering new avenues for securing the advantage and achieving mission success in the dynamic and contested theaters of future warfare.

BIBLIOGRAPHY:

1. al., A. Tripathi et. 2023. "End-to-End O-RAN Control-Loop For Radio Resource Allocation in SDR-Based 5G Network."
2. Bolas, E., G. Capela, and L. Bastos. 2021. "Protected core networking: communications challenges in tactical environments." 372-377.
3. Forces, SP's Land. 2019. *Tactical Communications: Evolving Technology.* https://www.spslandforces.com/story/?id=604
4. Ghosekar, Pravin, Girish Katkar, and Pradip Ghorpade. 2010. *Mobile Ad Hoc Networking: Imperatives and Challenges.*
5. Lucintel. 2024. "Tactical Communication Market Report: Trends, Forecast and Competitive Analysis to 2030." Lucintel.
6. One, Utilities. 2023. *The Role of Communication Satellites in Remote Military Operations.* https://utilitiesone.com/the-role-of-communication-satellites-in-remote-military-operations
7. Ryan, Mike. 2011. "A Case Study in the Utility of a Functional Architecture-The Tactical Communications System." https://www.researchgate.net/profile/Mike-Ryan/publication/270219365_A_Case_Study_in_the_Utility_of_a_Functional_Architecture-The_Tactical_Communications_System/links/54a33b720cf256bf8bb0e17f/A-Case-Study-in-the-Utility-of-a-Functional-Architecture-The-Ta
8. Salor, Laura, and Victor Baeza. 2023. *Harnessing the Potential of Emerging Technologies to Break down Barriers in Tactical Communications.*
9. Solutions, Mistral. 2020. *Tactical Communication Systems.* https://www.mistralsolutions.com/homeland-security/solutions/tactical-communications/
10. Suchanski, M., P. Kaniewski, J. Romanik, E. Golan, and K. Zubel. 2019. "Radio Environment Maps for Military Cognitive Networks: Deployment of Sensors vs. Map Quality."
11. Xiong, F., A. Li, and L. Tang. 2019. "An SDN-MQTT Based Communication System for Battlefield UAV Swarms."

1053477-3045-1396-24-26

CONSIDERATIONS FOR THE USE ARTIFICIAL INTELLIGENCE APPLICATIONS IN THE INFORMATIVE PREPARATION OF THE OPERATIONAL ENVIRONMENT IN MILITARY ART

Marian HOGEA, PhD. candidate
Colonel, Advanced Instructor, PhD candidate,
"Nicolae Balcescu" Land Forces Academy, Sibiu, Romania
E-mail: marianhogea1@gmail.com

Daniel ROMAN, PhD.
Colonel, Associate professor, PhD,
„Carol I" National Defence University, Bucharest, Romania
E-mail: Roman.Daniel@unap.ro

***Abstract**: The unprecedented technological development at the beginning of the 21st century was mainly attributed to the microelectronics, software, and networking industry, impacting all key areas of society: political, economic, military, social, and information infrastructures. Artificial intelligence applications hold a special place in this context, facilitating the scaling up of scientific knowledge and decoding the realities of the operational environment from a new perspective to predict crisis situations. Depending on the societal domain analyzed, the results of artificial intelligence applications have assumed new meanings in terms of proactive behavior, dedicated to command and decision components on all three levels: strategic, operational, and tactical.*

The informational preparation of the operational environment in military art has undergone substantial changes, encompassing the description of geographical areas, their economic and social potential, as well as understanding how military operations are influenced by identifying the complex of combat power multipliers and demultipliers. One of the major advantages of the results of artificial intelligence applications lies in the accuracy of details and the reduced time required to achieve objectives and develop solutions to military art problems, enhancing efficiency, innovation, and experience in solving crisis situations.

In the context of current military crisis situations, such as the war in Ukraine or the conflict in the Gaza Strip, Artificial Intelligence seeks to become a measuring, operational, and remedial tool at the disposal of researchers and decision-makers. In this article, we draw the attention of military specialists and beyond to the directions in which artificial intelligence applications can be exploited, offering not just a summary of possibilities, but rather a computer-aided working methodology for what we have called "Battle Smart – Command Center".

***Keywords:** military art, command center/post, artificial intelligence, resilience, societal, disruptive technology.*

Introduction – Military art in the technological context of the 21st century

Unprecedented technological development is the new reality of the 21st century in all areas of society, thanks to the possibilities of interconnection and unlimited information transfer, which generate a societal impact that is difficult to assess. The digitization of data and information has enabled the accumulation of databases and reference frameworks for the development of various phenomena over time, specific to societal domains. Thus, in the military field, technology has addressed several shortcomings in the development of military art across the spectrum: tactical, operational, and strategic. In this context, recent or ongoing military conflicts—such as the Nagorno-Karabakh war, the Russian-Ukrainian war, and the conflict between Israel and Hamas—clearly demonstrate the technological advantage in the battle space.

This is why there is talk of a radical transformation of 21st-century warfare, where technological weapons provide new meaning to military confrontation.

Under the impact of technology, the tactical component of military art has evolved into what is known as "smart defense," shifting from the "battlefield" to the "battle space". Weapons and weapon systems benefit from interconnection possibilities, making the targeting mix much more elaborate, and allowing decision-makers to plan and direct military actions in a computer-aided manner. At the tactical level, the presence of drones and artificial intelligence expands the capabilities of the "battle space" by conducting precise reconnaissance, gathering intelligence, and executing missions without the direct involvement of human troops. With increasingly advanced data analysis capabilities, artificial intelligence is becoming an essential tool for real-time decision-making, implying significant transformations in the way battles are fought and having a major impact on the military art of warfare.

I. Military art in the context of the technological battlefield – “the CD&E method”

Under the concept of the technologized battlefield, we observe a new dimension in the evolution of military strategy in the 21st century, emphasizing cyber warfare and the utilization of drones in military conflicts. Cyber-attacks have the potential to disrupt information systems, critical infrastructure, and influence geopolitical events. The widespread use of drones across military operations necessitates comprehensive reconsideration at tactical, operational, and strategic levels. Safeguarding against these threats and the capacity to counteract them have become primary concerns for modern armed forces and various societal sectors including political, economic, social, intelligence, and infrastructure. Military strategy across all spheres—tactical, operational, and strategic—introduces significant transformative elements in understanding the operational environment, particularly in deciphering the reality of the battlespace. A pertinent question arises concerning the technological implications, specifically regarding artificial intelligence in military conflict and its role in crisis management and alerting: "Can artificial intelligence address contemporary societal challenges? What are the implications of AI in the military sphere and, consequently, on military strategy?"

International bodies specializing in the evolution of military art such as NATO’s “Headquarters Supreme Allied Commander Transformation” are keeping an eye on the transformation of the battlespace and are regularly developing new concepts and appropriate tools to keep pace with the reality of the operational environment. In this respect we bring to attention “Concept Development & Experimentation (CD&E)” as a new way of work carried out in a “combination of methods and tools that stimulate NATO transformation, allowing the structured development of creative and innovative ideas into viable solutions”. [NATO, Concept development and experimentation, 2021, p. 3].

The methodology of conducting experimentation at the military art level through operational analysis transforms data obtained from the operational environment into working group-level inputs that formulate new concepts about methods, techniques, and procedures of warfighting. This facilitates the identification and integration of all types of threats, including cyber threats, and formulates solutions that are exploited in the area of protection of societal domains, the ones referred to above. The way of working developed by the “NATO CD&E community” is based on working facilitated by those technological, organizational, tactical, societal, or other developments that did not exist before or do not exist yet, in relation to the time of the formulation of the security problem or the reporting of a crisis situation.

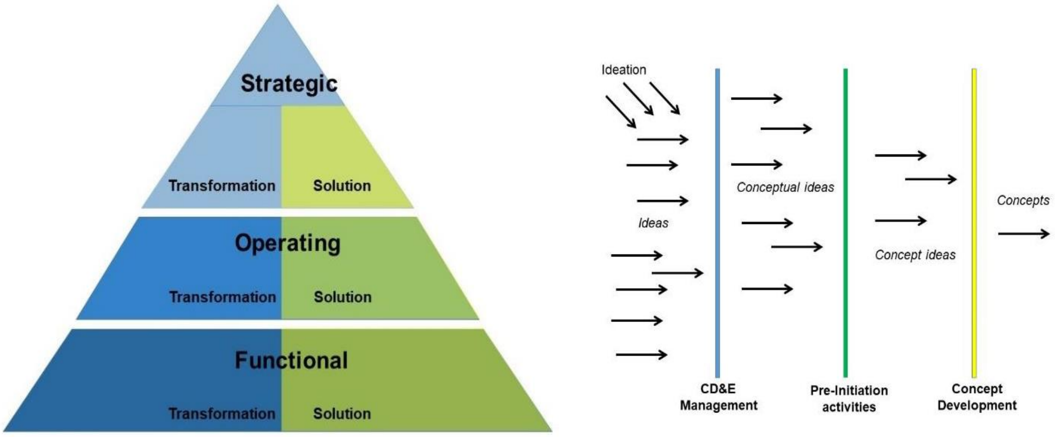


Figure no. 1. Graphical representation of the approach to operational analysis in the "Concept Development & Experimentation (CD&E)" Methodology [NATO, 2021, pp. 8-10)

The integrated and multi-disciplinary approach of the methodology in "Concept Development & Experimentation (CD&E)" allows for a realistic vision of the battlespace and, more than that, for a coherent construction of thinking on the three levels of military art: tactical/functional, operational and strategic, as in the graphical representation in Figure 1. It is important to note that the way of obtaining a new concept is based on the formulation of solutions to solve a problem, and this brings added value to the way of decision-making. In identifying the functionality of the working method, "the relation of ideas" is unidirectional and does not allow the feedback loop, as we are used to in systemic process analysis and knowledge. Therefore, we expect an evolution of the method of elaboration of concepts in a hermetic zone of scientific knowledge of phenomena and processes through a new relationship: goal, objectives and methodology of experimentation. This allows solutions to be developed in a purely innovative way that rejects any "source of conceptual blurring". The "CD&E method" is based on the analysis/investigation of the relationship between cause and effect, in which the aim is to identify the contributing factors influencing the expected results, formulated in a methodology-specific manner. Following the evolution and application of the "CD&E method", it is based on three types of experiments based on the "event": 1. analysis of the event by setting up its operational environment (construction of artificial systems), 2. introduction of the event in an ongoing exercise (real or simulation) and 3. The results of such a working method and the way solutions are obtained draw our attention to the concerns of defense and security specialists who are integrating advanced technologies into their work on conceptual areas, including military art, by involving artificial intelligence.

As a first conclusion, we can state that the evolution of military art under the impact of modern technologies is the result of an active process in which information resources are involved, whereby the notion of an event is exported to three distinct operational environments (artificially constructed, in an exercise and a real situation) and the results are transformed into new concepts with different implications at the level of military art: tactical, operational and strategic.

II. The informative preparation of the operational environment under artificial intelligence

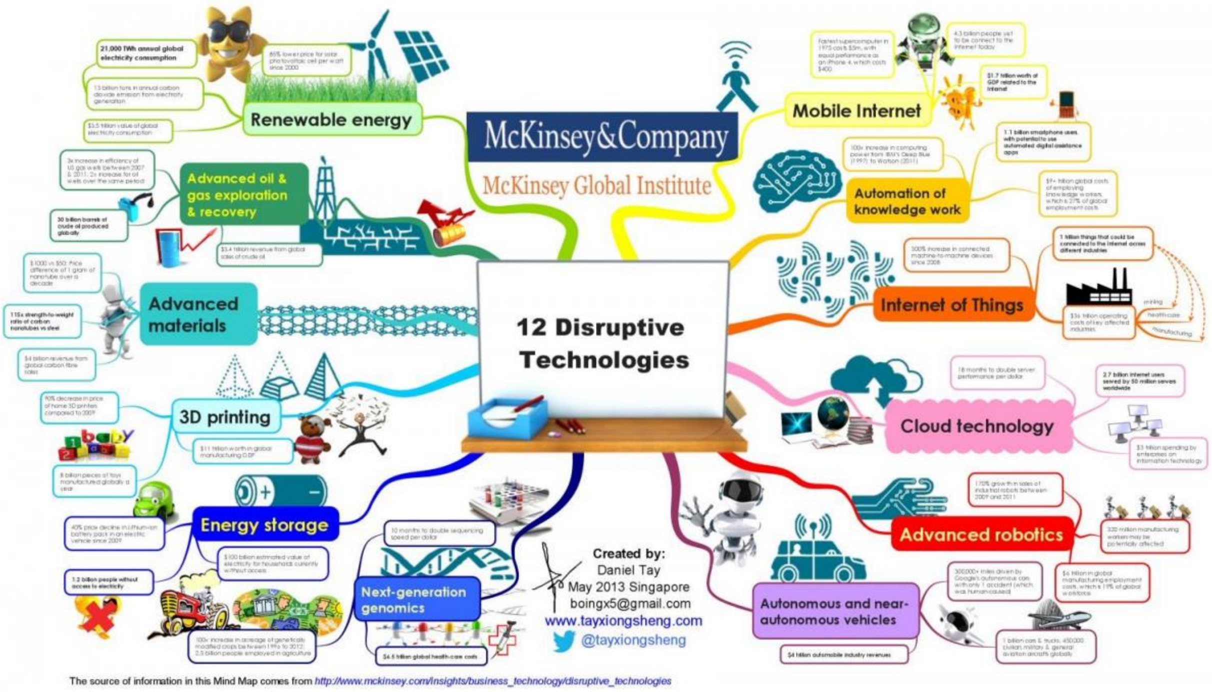
Military art, a fundamental component in the toolkit for resolving a military crisis situation, is the "cornerstone" in the preparation and implementation of defense and retaliation solutions in the face of a hypothetical adversary. Knowing and understanding the "CD&E

method" allows us to open new horizons in decoding the reality of the contemporary operational environment and understanding current military conflicts: the Russian-Ukrainian or Israel-Hamas war. The introduction of the "event" in an experimental context allows us to understand the operational environment at a higher level. During the development of the method, a series of iterations take place, describing or incorporating elements of the crisis into a much broader picture of situations, thus determining the characteristics of a future situation with pre-established implications for the subject under analysis. In this way, we can state that military art goes beyond its framework of resolving a military conflict and can make predictions about states of crisis or military nature that may include the engagement of forces at the tactical level.

In this equation of crisis resolution, we conceptually identify the role of disruptive technologies (Bower, Christensen, 1995, pp. 47-49). Disruptive technology is a term coined at Harvard University by business school professor Clayton M. Christensen who used the term to describe a new technology that unexpectedly replaces an established technology in a particular field (Clayton M. Christensen, 2020, p.2). In this idea, we identify the shifts that have taken place in the military art from "battlefield" to "battle-space" a conceptual means of linking materially, behaviorally, cognitively and geographically all aspects of armed confrontation. In this sense we identify on the same conceptual line of military art, the term "Battlespace Management", which in most cases, depending on the level of reporting, tactical, operational or strategic the notion of management is preferred to the notion of military art (NATO, JDP 3-70, 2019, pp. 11-19). In this context, another observation is related to the coherence of the concepts of "Battlespace Management" and "operational art" without distinguishing their role in relation to military art. The transition from the tactical level of individual weapons or weapon systems within force categories (land forces, air forces, naval forces) to the combined arms level has been achieved through the assimilation of new concepts such as "joint" and "multi-domains". In this context, is it possible to talk about the existence of disruptive technologies at the level of military art? And if so, how exactly have they been taken up and what are the effects of these conceptual changes?

The presence of disruptive technologies in military art can be seen as a new stage in its development, a true startup in its three components: tactical, operational and strategic. In this context, the information preparation of the operational environment takes on new dimensions that, when translated into the coordinates of disruptive technologies, radically transform the decision-making environment, a fundamental characteristic of command and decision points/centers. The cumulative decision at the level of each category of force becomes a convergent joint decision and has the character of multi-domains. This allows us to make a conceptual comparison of the concept of "smart". As an example, we will choose a complex societal model of the "smart" type such as an urban community, i.e. a "smart city" concept in which we will look at the initiation, rationale and adoption of the decision. Since 2008, summaries of disruptive technologies with major geopolitical, military, economic, social and industrial implications have been prepared. The "smart city" concept is the result of practical and conceptual implementations of disruptive technologies, synthetically presented according to the Clayton M. Christensen model as in Figure 2.

By linking the two concepts, we identify that disruptive technologies and the smart city concept are interlinked in the sense that disruptive technologies can play a significant role in transforming cities into more efficient and resilient so-called "smart cities". A smart city is a concept that refers to the use of technology and data to improve efficiency, sustainability, quality of life and resource management in a city, and, more than this, by introducing feedback and feedforward cells respectively, a new perspective can be achieved at the conceptual level of dealing with a crisis situation. In order to highlight the relevant aspects regarding the concept of "smart city – resilient", we will refer to: the Internet of Things (IoT), smart mobility generated by autonomous transport vehicles, smart energy management systems, digital information platforms, artificial intelligence support in decision-making modules (Samarakkody, Amaratunga, Haigh, 2023, pp. 6-14). The resilience of such a community based on disruptive technologies is generated by a multitude of aspects such as: managing emergency situations, achieving an extended, connected and efficient infrastructure, communication and early warning for unforeseen situations, generating data and predictive analytics to assess and anticipate potential risks, last but not least, informing and connecting the community on the evolution, through monitoring, of a crisis situation.


McKinsey&Company
McKinsey Global Institute
12 Disruptive Technologies
Renewable energy
21,000 TWh annual global electricity consumption
13 billion tons in annual carbon dioxide emission from electricity generation
$3.5 trillion value of global electricity consumption
85% lower price for solar photovoltaic cell per watt since 2000
Advanced oil & gas exploration & recovery
3x increase in efficiency of US gas wells between 2007 & 2011; 2x increase for oil wells over the same period
30 billion barrels of crude oil produced globally
$3.4 trillion revenue from global sales of crude oil
Advanced materials
$1000 vs $50: Price difference of 1 gram of nanotube over a decade
115x strength-to-weight ratio of carbon nanotubes vs steel
$4 billion revenue from global carbon fibre sales
3D printing
90% decrease in price of home 3D printers compared to 2009
$11 trillion worth in global manufacturing GDP
8 billion pieces of toys manufactured globally a year
baby
Energy storage
40% price decline in lithium-ion battery pack in an electric vehicle since 2009
1.2 billion people without access to electricity
$100 billion estimated value of electricity for households currently without access
Next-generation genomics
10 months to double sequencing speed per dollar
100x increase in acreage of genetically modified crops between 1996 to 2012; 2.5 billion people employed in agriculture
$6.5 trillion global health-care costs
Created by:
Daniel Tay
May 2013 Singapore
boingx5@gmail.com
www.tayxiongsheng.com
@tayxiongsheng
Mobile Internet
Fastest supercomputer in 1975 costs $5m, with equal performance as an iPhone 4, which costs $400
4.3 billion people yet to be connect to the Internet today
$1.7 trillion worth of GDP related to the Internet
Automation of knowledge work
100x increase in computing power from IBM's Deep Blue (1997) to Watson (2011)
1.1 billion smartphone users with potential to use automated digital assistance apps
$9+ trillion global costs of employing knowledge workers, which is 27% of global employment costs
Internet of Things
300% increase in connected machine-to-machine devices since 2008
1 trillion things that could be connected to the Internet across different industries
$36 trillion operating costs of key affected industries
mining
health-care
manufacturing
Cloud technology
18 months to double server performance per dollar
2.7 billion internet users served by 50 million serves worldwide
$3 trillion spending by enterprises on information technology
Advanced robotics
170% growth in sales of industrial robots between 2009 and 2011
320 million manufacturing workers may be potentially affected
$6 trillion in global manufacturing employment costs, which is 19% of global workforce
Autonomous and near-autonomous vehicles
300,000+ miles driven by Google's autonomous cars with only 1 accident (which was human caused)
1 billion cars & trucks, 450,000 civilian, military & general aviation aircrafts globally
$4 trillion automobile industry revenues

The source of information in this Mind Map comes from http://www.mckinsey.com/insights/business_technology/disruptive_technologies

Figure no. 2. Graphical representation of the implications of disruptive technologies as implications and transformations in different societal domains
(McKinsey – 12 disruptive technology)

Following the "smart city" model, the presence of disruptive technologies in the military decision-making area is achieved through elements of disruptive technology that are integrated into a command point/decision center, resulting in the possibility of achieving a more agile, informed and efficient operational ensemble, adapted to the challenges of today's operational environment. Military art in this new context of the application of disruptive technologies, under the impact of artificial intelligence, takes on new meanings, as we have said, in the area of situation and crisis prediction in particular.

Under the impact of disruptive technologies, the military decision-making area involves a new dimension of information readiness of the operational environment, a crucial aspect of the planning and execution of military actions and operations, as the ability to obtain and interpret information in real-time can decisively influence the outcome of a military conflict. The involvement of disruptive technologies in the process of analysis and information preparation of the operational environment identifies in real-time and in advance the sum of the factors influencing military actions and operations, thus highlighting the multipliers and demultipliers of combat power. In this context, we appreciate that the integration of artificial intelligence in the analysis of combat power multipliers and demultipliers brings with it a more dynamic and informed approach in the military domain, contributing to increased efficiency, adaptability and operational capabilities, aspects that essentially support the concepts of “Smart Defense”, “Battlespace Management” or “multi-domains”.

For the relevance of the enhancement of the results of the informative preparation of the operational environment at the level of a command point, we will refer to the way of obtaining the influence factors, i.e. the multipliers and demultipliers of the combat power under artificial intelligence with direct impact on the resilience of the entity in question. In this respect AI distinguishes between the two categories of factors with a focus on combat power multipliers in four distinct categories: 1. - surveillance and reconnaissance in the confrontation space, 2. - performing predictive analysis, 3. - AI-assisted decision making and 4. the possibility of advanced simulations of possible situations. The integration of combat power multipliers into the process of intelligence preparation of the operational environment involves: 1. - identification of vulnerabilities, 2. - cyber security situation, 3. - analysis of logistical resources and 4. - analysis of combat strategies, tactics and techniques/behavior patterns of a potential adversary. The integration of such capabilities requires the reconfiguration of the decision center, i.e. the point of command.

III. “Battle Smart – Command Center” a solution for integrating artificial intelligence capabilities in planning and conducting military actions/operations

The role of the decision center, the command point, is essential in planning and conducting military actions and operations. The basis of how the act of decision and command is conceived and carried out is the military art with all its strategic, operational, and tactical components. Starting from “Concept Development & Experimentation (CD&E)”, a new way of working achieved through a “combination of methods and tools that stimulate NATO transformation, enabling the structured development of creative and innovative ideas into viable solutions” we have extrapolated the methodology to the reconsideration of the role and way of working of the decision center, i.e. the command point.

From a different perspective, adopting the concept of the 'smart city' and applying the necessary capabilities of the 'Battlespace Management' concept, we have named the new concept the 'Battle Smart - Command Center' as a command point/decision center. The integration of disruptive technologies across the three levels of military art radically transforms the way military confrontation is conceived and assigns a new role to the resilience of the entities involved. The use of combat power multipliers in the planning process translates military art through integrated decision-making following the Boyd model into the OODA feedback loop, as shown in Figure 3. This results in mutations in the quality of the values obtained at the command point or decision center between the two variants: the 'traditional operating model' and the 'digital operating model.' The implications of Artificial Intelligence are that OODA processes run much faster from one stage to the next, and the quality of the products produced by the feedback loop is significantly improved. Introducing data analysis algorithms into the feedback loop using AI enables massive analysis and interpretation of datasets to identify trends, patterns, and forecast enemy movements and actions. This facilitates 'smart' predictive analysis, where sensor results from the battlespace are processed and solutions to tactical, operational, and strategic-level problems become anticipatory. AI can offer quick and accurate recommendations to commanders based on the analysis of available data, contributing to more informed and effective decision-making. Furthermore, by involving AI, hypothetical future situations can be projected and events simulated to help avoid losses and crisis situations. The use of AI in complex simulations can provide a deeper understanding of the interactions between one's own forces and those of the adversary, enabling the testing of different scenarios for engaging forces or avoiding pitfalls and unnecessary losses. Identifying combat power multipliers in the planning process through a 'what-if' analysis highlights risk-generating situations by identifying vulnerabilities and quantifying threats and courses of aggression from the adversary.

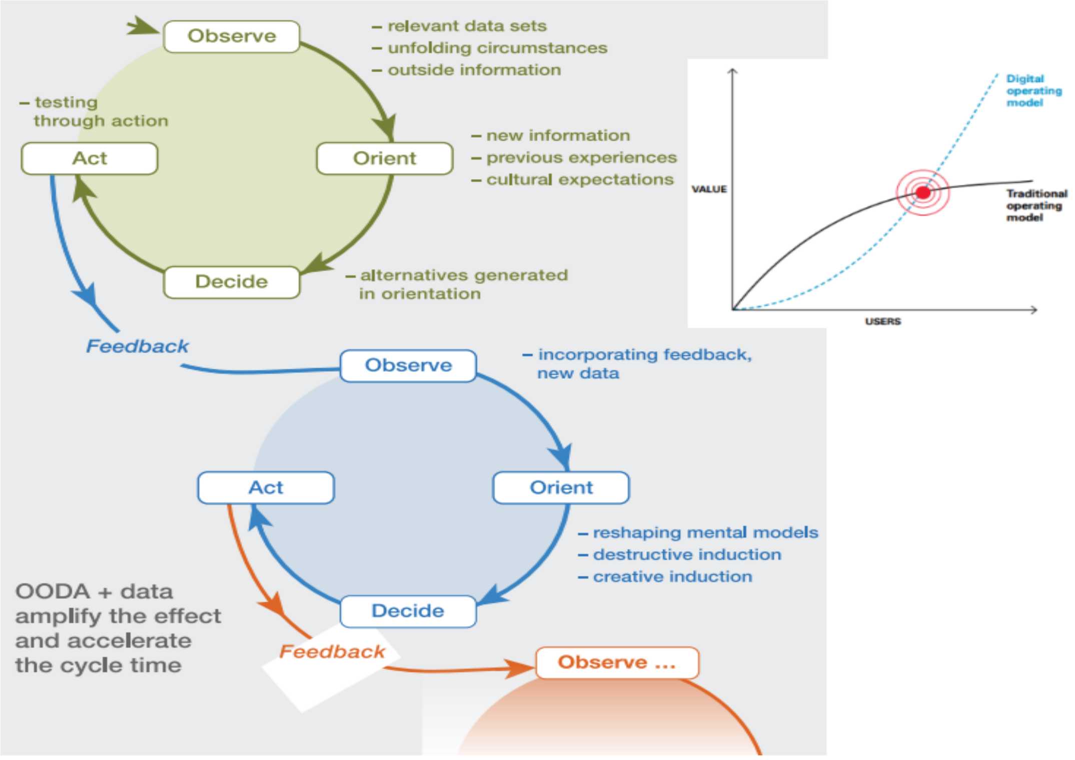


Figure no. 3. Graphical representation of OODA decision-making by feedback loop under AI (Mayhew and Co, 2017, p. 83)

The integration of disruptive technology applications in the act of decision and command, the involvement of artificial intelligence in military art, leads to an automation of processes: observe, orient, decide, act, freeing human resources for more complex and strategic activities based on personal feeling and experience. In this way, the "digital operating model" values the results obtained in the process of planning and conducting military actions/operations as far superior to the "traditional operating model", which implies the opening of new perspectives of military art.

Conclusions and proposals

The first conclusion is related to how contemporary societies evolve under the impact of disruptive technologies and their implications in all societal domains: political, military, economic, social, information, and infrastructure. The efforts of NATO specialists to identify new concepts for the development of the decision-making and command framework have highlighted new working methods and methodologies such as "Concept Development & Experimentation (CD&E)". The mechanisms of such methods and methodologies can be exported to all societal domains, and "smart" mutations can take place that radically transform the way we decode the reality of the operational environment.

Another conclusion relates to how disruptive technologies have permeated everyday life in all societal domains, including the military, and are leveraging their capabilities by managing resources at a higher level of data processing speed and refining them through feedback loops. In this context, military art becomes predictive in the sense that the actions of a hypothetical adversary can be anticipated and, moreover, can be engaged at an early stage through appropriate measures at a resource cost appropriate to the situation of prevention rather than crisis. In the light of the concepts of “Smart Defense”, “Battlespace Management”, or “multi-domains”, military art is progressively expanding from the level of independent activities to their synchronization and ultimately to their integration in a coherent and unified manner. This also involves a shift in control methods from procedural to dynamic procedural and the activation of deconflictions so that, in the end, only positive results can be achieved.

Operating combat power multipliers and demultipliers with artificial intelligence transforms the capabilities of classical (traditional) decision centers/command points into a new set of predictive modelling-simulation capabilities. In this context, the Battle Smart - Command Center concept is more of a solution to the current challenges and reality of ongoing military conflicts. Without smart weapons, military actions can no longer be carried out and their absence generates significant loss of life and material damage.

In our opinion, studying how new concepts related to military art are generated will allow us to understand the essence of the transformations at the procedural level and, moreover, will help us realize our own organization of decision-making and action. We suggest that decision-makers analyze the possibilities of identifying and integrating disruptive technologies at the level of decision centers and command points. At the same time, we recommend greater attention to obtaining and exploiting data and information from the operational environment to exploit combat multipliers and demultipliers.

Even if we have only referred to the conceptual level, “Battle Smart - Command Center” can be a solution to the challenges of today’s operational environment that allows the exploitation of disruptive technologies and, as a result, the resilience of entities to be enhanced. In conclusion, we express our conviction that addressing the topic of “smart” at the level of military art, by bringing attention to the disruptive technologies present in all societal domains, is a first step towards identifying the solutions necessary to redesign the engagement of forces in a hypothetical military conflict as well as to engage in resolving crisis situations.

BIBLIOGRAPHY:

1. Boudreaux-Dehmer Manfred, ‘Innovation and the Digital Transformation’, NITECH: NATO Innovation and Technology, vol. 9, July 2023, p. 17, https://issuu.com/globalmediapartners/docs/nitech9_-_full_pdf_final?fr=xPf81NTU
2. Bower L. Joseph, Christensen M. Clayton, Disruptive Technologies: Catching the Wave, Harvard Business Review Notice of Use Restrictions, 1995, (In-text citation: Bower, Christensen, 1995, pp. 47-49)
3. Mayhew Helen, Saleh Tamim, Williams Simon, Making data analytics work for you—instead of the other way around, Introducing the next-generation operating model McKinsey on Digital Services, 2017, (Mayhew and Co, 2017, p. 83)
4. Polomé Didier (Brig.-Gen.), ‘Alliance Digital Transformation for Multi-Domain Operations’, NITECH: NATO Innovation and Technology, vol. 9, July 2023, p. 39, https://issuu.com/globalmediapartners/docs/nitech9_-_full_pdf_final?fr=xPf81NTU
5. Samarakkody Aravindi, Amaratunga Dilanthi, Richard Haigh, An Exploration of Emerging and Disruptive Technologies for Improving Disaster Resilience in Smart Cities: An Urban Scholar’s Perspective, 2023, doi: 10.20944/preprints202306.1091.v1, . (In-text citation: Samarakkody, Amaratunga, Haigh, 2023, pp. 6-14)
6. Slitine Marion, Contemporary art from a city at war: The case of Gaza (Palestine), 2017, https://hal.science/hal-03059302/document
7. Sydorenko Andriy, Chibalashvili Asmati, Ukrainian digital art during the full-scale Russian-Ukrainian War, 2023, DOI:10.33543/j.130237.125130

8. Voda, A.I.; Radu, L.D. How can artificial intelligence respond to smart cities challenges? In Smart Cities: Issues and Challenges; Amsterdam, The Netherlands, 2019; pp. 199–216
9. Xinyi Gu, Jun Qiu, Jing Cao, Zimo Ge, Zhe Wang, Design of an Evaluation System for Disruptive Technologies to Benefit Smart Cities, 2023,
10. NATO, Concept development and experimentation, A concept Developer`s toolbox, 2021, (NATO, Concept development and experimentation, 2021, p. 3)
11. NATO, Joint Doctrine Publication 3-70, Battlespace Management, 2019 (In-text citation: NATO, pp. 11-17)
12. NATO, 'NATO Allies Take Further Steps Towards Responsible Use of AI, Data, Autonomy and Digital Transformation', 13 October 2023, https://www.nato.int/cps/en/natohq/news_208342.htm
13. https://vogue.ua/battlefrontukraine/index-en.html
14. https://static.rusi.org/202303-SR-Unconventional-Operations-Russo-Ukrainian-War-web-final.pdf.pdf
15. https://cmeil.gmu.edu/wp-content/uploads/sites/50/2023/11/Wheatley_LOAC_FINAL.pdf
16. https://jinsa.org/wp-content/uploads/2023/12/Israels-Operation-Swords-of-Iron-Update-12-18-23-2.pdf

SECTION 3

MULTI-DOMAIN OPERATIONS, RESOURCES MANAGEMENT AND OGISTICS

1053477-3045-1396-24-27

CAN MULTI-DOMAIN INTEGRATION BE THE RESPONSE TO HYBRID THREATS? ARGUMENTS AND COUNTER-ARGUMENTS

András MEZŐ, PhD.
Lieutenant Colonel, lecturer, military sciences, Ludovika – University of Public Service,
Budapest, Hungary
E-mail: mezo.andras@uni-nke.hu

Mariann TÁNCZOS, PhD.
Captain, assistant lecturer, military sciences, Ludovika – University of Public Service,
Budapest, Hungary

***Abstract**: The vision of the multi-domain operations (MDO) concept, which promotes the principles of Unity, Interconnectivity, Creativity, and Agility, is to prepare, plan, orchestrate, and execute synchronized activities across all domains and environments at scale and speed in collaboration with other instruments of power, stakeholders, and actors. This delivers tailored options at the right time and place that build advantage in shaping, contesting, and fighting and present dilemmas that decisively influence the attitudes and behaviours of adversaries and relevant audiences. The vision raises the question of whether the idea can be used to counter hybrid threats. The study employs comparative analysis to investigate the potential applications of the MDO concept in combating new multifaceted threats, such as hybrid warfare. The preliminary findings indicate that MDO is not only a more complete concept that can be successfully applied to a larger range of difficulties but also a suitable response to hybrid threats.*

***Keywords:** multi-domain operation, multi-domain integration, hybrid threats, all-government approach, new and emerging threats, asymmetric threats.*

Introduction

The operational environment for NATO has been fundamentally altered by the ongoing great power competition across all domains and environments, the pervasive global insecurity, a series of crises, and major strategic shocks of the recent past. The illegal annexation of Crimea in 2014, the constant tension in the Taiwan strait, the war between Russia and Ukraine since 2022, and HAMAS and Israel since 2023, and the rise of ISIS and al-Quaeda in the Middle East and North Africa all indicate the start of a new era in military thinking as well. Today's multifaceted threats from all strategic directions in an increasingly complex, hyperactive, urbanized environment with no geographical boundaries and where competition and contestation between parties in all domains are taking place needed new answers and approaches from military thinkers to provide adequate answers to the emerging new challenges. Operations in cyberspace and outer space have an increasing impact on security and how it is perceived, which requires a radical transformation of military thinking. Cyberspace has effectively become a battleground for fighting below the constant threshold of war (Strucl 2022, 113.), and there is increasing competition in space (Paikowsky, 2021).

The first multi-domain operation (MDO) doctrine was released by the US Army in 2018 (TRADOC, 2018). It was not the start, but the result of a new operating concept. From being a single NATO Member State strategy MDO spilled over into the strategic thinking of other Member States, like, the United Kingdom, Spain, and even in the smaller states, like Hungary.

As a new concept, there are always debates around the opportunities and ways of its practical usability. In this paper we focus on the MDO concept's possible operationalization in just one segment, namely hybrid threats.

It must be acknowledged that even if kinetic military strikes continue to dominate conflicts, it is increasingly clear that they will no longer be fought exclusively on sea, land, and air in future conflicts. Nor do they necessarily have to have lethal consequences to achieve their objectives. Military operations increasingly rely on space and cyber capabilities, which pose an invaluable threat. *The Alliance must prepare for these new threats, regardless of whether they are labeled asymmetric, hybrid or fourth-generation warfare.*

I. Methodology

The paper utilises the framework of comparative analysis methodology to establish if MDO could provide an adequate answer to hybrid challenges. Since the paper investigates the adaptability of MDO as an answer to hybrid threats the methodology cannot be applied in its original form. Ragin designed qualitative comparative analysis especially to describe complex cases with multiple sets of comparable cases (Ragin 2014, 1-18). In this case, no complex cases will be examined, but two concepts. Despite the topic's loose connectedness to the original methodology, comparative analysis can be applied. Multiple scholars describe it as one of the basic methodologies of political sciences (Sartori 1970, 1033; Lijphart 1971, 682; Pickvance 2001, 10), thus its utilization has legitimacy.

Comparative analysis can be described as a method which describes causal relations between two or more cases. Thus, this method can be approached from two aspects, namely the differences or similarities of the selected cases (Pickvance 2001, 10-11). Present research attempts to explore a theoretical relationship between MDO and hybrid, which validates the utilisation of the selected methodology. Throughout the paper, the definition of the MDO concept, accepted by NATO in 2023 is regarded as the independent variable. The research will present and analyse both the similarities and differences of MDO and hybrid concepts, exploring the applicability of the first one in the case of the latter.

In this regard, the two most important concepts for the research are the MDO concept of NATO, and the hybrid threats definition of the NATO. Thus NATO describes MDO as the following: *The orchestration of military activities, across all domains and environments, synchronized with non-military activities, to enable the Alliance to create converging effects at the speed of relevance* (ACT 2023). As well, NATO defined hybrid warfare threats in 2014 *where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design* (NATO 2014). Later, the organisation rephrased slightly its original definition as *a type of threat that combines conventional, irregular and asymmetric activities in time and space* (NATOTerm w.y.). For the research the two latter definitions are treated as one.

II. Literature Review

Although MDO concept is relatively new within NATO, it is not an entirely new concept within the realm of military science. Literature can be found from as early as 2003 on the topic, when MDO meant the integration of four domains, land, sea, aerospace and cyberspace to answer new challenges, which were described as uncertainty, initiative, and jointness (Gompert 2003, 1). The US Army and Air Force used different expressions to describe it, like cross-domain and joint all-domain, and treats it as an extension of the joint operations to cyberspace and space (TRADOC 2018; AETC 2020). Regardless of this oversupply of expressions to describe the very same concept, the general view on MDO is that it is the natural evolution of the joint-force operations to meet future challenges and ensure success (Bott 2017; Townsend 2018, 1-2, Hegedűs and Hennel 2020, 4; Fazekas 2022, 60). Despite MDO concept's recent appearance in military thinking, the literature on it is already very extensive, revolving around the need for a new concept (Balboni et al. 2020, 17-32), the explanation of the new strategy (Wille 2019, 9-12) the complexity of it (Carlisle 2017, 4-5), and how to operationalize different aspects within MDO concept (Andreski and Taliaferro 2019).

According to the sources, it is not an uncharted territory to argue if hybrid threats can also be addressed in the realm of MDO concept. Viewpoints on the outcome of the argument are not uniform. Those works, which focus on the MDO concept strictly from the military point of view, using the 2018 TRADOC doctrine as their main source are tend to be more skeptical on MDO's applicability, however they acknowledge its potential as an appropriate tool. These works either contest the concept's feasibility (Stafford 2019, 100-101) or its budgetary demands versus its benefits (Kang, 2020, 102-105). Literature, which considers MDO from the hybrid warfare perspective is more permissive and generally call for an all-government approach of the MDO. These works claim, that MDO has to include non-military aspects as well (Cordesman and Hwang 2020, 12-13; Jones and de Leon 2020, 41). From the perspective of hybrid warfare, it is reference on its multi-domain nature, but the connection was not made yet (Schmid 2020). This indicates that debate on this question is still valid and timely.

III. MDO according to NATO definition

The MDO concept is not just a recognition of two new domains of operations (cyberspace and space), indeed MDO is more than just (military) operations in all five domains at the same time. MDO makes the broad political and military strategy a reality, while also using all the instruments of power (diplomatic, economic, information) and allowing the Alliance to integrate the separate multi-domain capabilities of the Member States and their armed forces into *a joint multi-domain operation*.

The NATO MDO concept focuses strictly on military objectives and the use of military force but recognizes that military success depends on the cooperation of multiple actors, and therefore much greater emphasis needs to be placed on cooperation, coordination and synchronization (Mező 2022). MDO requires a new philosophy and a data-driven and creative mindset that can plan and act comprehensively across all five operational domains. For MDO to succeed, nations themselves must embrace a much broader data sharing and federation-wide data use than ever before.

NATO member states' military capabilities need to be updated, new concepts and doctrines are needed to enable offensive and defensive operations in all five domains. The development of such capabilities in some domains may seem unlikely at the moment, but their necessity is indisputable. For example, offensive capabilities are needed not only in the traditional operational domains (land, aerospace, maritime) but also in the two new key domains (space and cyberspace). Without offensive capabilities in space and cyberspace domains, we risk ceding these two to the enemies and these domains link the other three, thus making our capabilities isolated and easy to counter. The dominance of space and cyberspace will be vital to NATO, the superiority gained in these two domains does not necessarily mean victory over the other three spaces, but their loss is certainly a defeat. (Mező, 2020)

III.1 The details of the MDO concept

MDO is focused on achieving military objectives across all domains and environments, but recognizes that there were many actors that collectively contribute to military success, such as the instruments of national power (IoP), including commercial entities, and other stakeholders whose role may be critical to the success or failure of a military operation. At the operational level, these IoPs are not available, but the NATO Multi-domain Task Force (MD TF) Commander consults and synchronizes his operational plans with them and seeks full collaboration. The coordination and synchronization of these military and non-military activities will enable delivering converging effects. Converging effects are effects of such magnitude, achieved simultaneously or in rapid succession, that the sum of the effects is greater than the sum of the individual effects. Note that the tailored options may not always have the traditional lethal effects. NATO forces must use intermediate means (non-lethal directed energy, cyber, electronic warfare, information operations, and other pertinent capabilities) that deliver effects beyond presence but below the threshold of lethal force to prevent disproportionate or unintended effects (excessive incidental losses, collateral damage), and adversaries' negative narratives.

III.2 Description of the MDO concept

NATO's agreed MDO concept has four core principles: *unity, interconnectivity, creativity and agility* (ACT 2022). These principles have evolved from and are not in contradiction with those of the joint operation, and better articulate them for the application of cyberspace and space capabilities.

Unity: The unity of MDO forces enables the coordinated deployment of all capabilities towards a common goal, while providing a basis for the coordination of military activities and the synchronization of non-military capabilities. Coordinated MDO planning and execution requires collaboration between nations, trust, transparency and bridging differences in perspectives.

Connectivity: The interconnectivity of MDO forces helps to understand the situation and share the knowledge gained. Interconnectivity is hampered by the technology gap between legacy and modern platforms and interfaces, interoperability issues, and data classification and privacy, so the digital architecture of the future must be flexible, resilient and highly standardized to support user requirements.

Creativity: The creativity of MDO has limitless potential to surprise and confuse the enemy. The creativity of leadership relies on the ability of the commander and the staff to analyze complex situations from new and unusual perspectives and to recognize simple solutions and opportunities deep within them. Creativity is fostered by the simple visual representation of the situation and its complex interrelationships.

Agility: The agility of operations allows MDO forces to exploit fleeting opportunities, take initiative, anticipate enemy by collecting data faster, prioritizing tasks, dynamic tasking and autonomous, decisive action. Agility requires flexibility of thought and action from both superiors and subordinates.

The implementation of these principles requires the creation of a digital network. This is a new structure, which acquires, manages, analyzes, evaluates, exchange, and share vast amounts of data and will ensure the MDO principles are implemented and NATO MDO forces are connected from the tactical level all the way up to the strategic level. The digital network will ensure the synchronization of the activities of the MDO forces with other components and systems of the national IoP of the Member States, as well as the possibility of consultation and cooperation with other actors (e.g. commercial service providers, private satellites, etc.). The system must be robust, resilient and able to adapt to changes in technological developments.

IV. Discussion

To conduct the comparative analysis, first, the definitions of MDO and hybrid warfare threats are assessed point by point. Subsequently, cross cutting issues are examined, being taken into consideration through the lens of hybrid warfare. The analysis lists firstly the arguments for (subparagraphs a.) and then the arguments counter (subparagraphs b.) to assess MDO's adaptability against hybrid warfare.

1. MDO's adaptability against hybrid warfare.
   a. NATO's MDO concept claims that it has to adapt both military and non-military activities to answer challenges. Hybrid warfare threats are by NATO's own definition military, paramilitary, and civilian measures. The statements related to the nature of activities reveal a highly compatible setting for our argument. According to this, MDO can be NATO's (the West's) response to the Chinese and Russian hybrid threats. In other words, NATO will be able to provide adequate responses adapted to the nature of the hybrid warfare.
   b. The USA is the only country that has already applied the MDO concept which was developed in response to hostile regular armies' (namely China and Russia) and their anti-access/area denial (A2/AD) systems (TRADOC, 2018). It is therefore not appropriate to claim that NATO has created its concept to counter hybrid warfare because the MDO concept serves different purposes and offers a pathway to address more general challenges. NATO has interpreted the problem much more broadly to meet the diverse expectations of its Member States.
2. MDO is very similar to hybrid warfare.
   a. The MDO concept claims that it has to plan its activities across all domains (land, sea, aerospace, space, and cyberspace). While the hybrid warfare threats definition is less exact on this matter, it states that activities are combined in time and space. As Schmid (2020, 2.) claims, hybrid warfare can combine multiple non-military dimensions including politics, information, economy and technology, complementing the more traditional military domains. On this account, the MDO concept can provide a strategic tool to be able to respond to hybrid warfare threats. It is however only possible if an all-government approach is followed throughout the implementation of the concept as well.
   b. Yet, the definition of 'hybrid' does not mean per definition *covert*, but it is very much an inherent part of the hybrid threat, to hide the identity of a perpetrator when delivering effects. The cyber domain allows a more effective area where actions take place that can be more easily concealed, in some ways like Special Forces operate. Deniability can be useful, especially below the threshold of war.
3. Hybrid threat is time sensitive.
   a. Regarding hybrid threats, time is a key element in the response. For this, NATO has to be capable of recognizing it. This element is key in this argument, since the already existing NATO Early Warning System has the capabilities to recognize a hybrid attack against the Alliance if it is calibrated properly. Time is and was always an important factor, and the MDO concept recognized the need to "create converging effects at the speed of relevance" also. The speed of military actions in space and cyber requires an accelerated, automated and AI enabled decision making process.
   b. Timeliness can be a question however when it comes to NATO answers. As an international organization with 30 some members the decision making process can be slow and bureaucratic. In the case of hybrid threats article V. cannot be evoked, which can make the decision-making process even slower, and the organization can lose initiative.
4. MDO is the new comprehensive approach.

   a. In the comprehensive approach we seek to ensure unity between all instruments of power to achieve a collective solution. Diplomatic discussions, economic trade sanctions, the exposure of false adversary narratives, and the deter and defend actions of the military forces can all occur in isolation under the responsibilities of different departments, but all will ultimately contribute to the comprehensive approach.
   b. NATO’s MDO is military focused and does not seek to replace the intent of a comprehensive approach. MDO is the military contribution to a comprehensive approach and is primarily concerned with achieving military objectives that support the Alliance’s political aims. MDO is focused on achieving military objectives and is the MIoP’s contribution to the comprehensive approach.

5. MDO is the new joint operation.
   a. Joint operations are military activities carried out by combined forces and specific service forces operating, which do not independently constitute joint forces. A joint force is a military unit made up of substantial components from two or more services, working under a single joint force commander. Joint operations are the main method used by modern armies and from this perspective MDO means no big difference.
   b. Joint was focused on the forces of the Army, Air Force and Navy and an operation that involved two or more of these forces, was classed as joint, irrespective of what operational domains they were operating in. MDO is focused on the domains, irrespective of the forces assigned. Some Armies have air assets, counter-space assets, and land assets, therefore can operate in multiple domains without other services. In short every joint must be MDO, but not every MDO is joint.

Conclusions

The Alliance’s approach to MDO will enable NATO’s Military IoP to prepare, plan, orchestrate, and execute synchronized activities, across all domains and environments, at scale and speed in collaboration with other IoP, stakeholders, and actors. This delivers tailored opinions, against not only hybrid threats but also asymmetric, hybrid or fourth generation warfare as well. While the MDO concept and hybrid warfare both involve planning operations across multi-domains and may leverage civil capabilities, the significant difference lies in the clandestine nature and deniability of the hybrid threat. NATO cannot risk any dubious operation, that would undermine its credibility.

Time is crucial in responding to hybrid threats, and NATO must recognize them using its Early Warning System. The MDO concept emphasizes creating converging effects at the speed of relevance. However, NATO's slow and bureaucratic decision-making process, especially in the case of hybrid threats, may hinder its ability to respond effectively.

Meanwhile comprehensive approach seeks to ensure unity between all IoP to achieve a collective solution, MDO is the MIoP’s contribution to the comprehensive approach. It goes beyond joint operations, transcends it, and ultimately replaces it, undoubtedly.

BIBLIOGRAPHY:

1. ACT. 2022. Alliance Concept for Multi-Domain Operations. ACT, Norfolk, 2022. (SH/SDP/SDF/TT010038)
2. ACT. 2023. AJP-3.27 edition A, version 2 Allied Joint Doctrine For Counter-Insurgency. (COIN). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1154495/20230503-AJP-3_27_COIN_EA_V2-O.pdf. Last modified 2023. (In-text citation: AJP-3.27)
3. ACT. 2023. Validated Concept 0.9, Operating Concept for Multi-Domain Operations in the Urban Environment, ACT, Norfolk, 2023. (In-text citation: MDO UE concept, 2023)
4. AETC. 2020. "Air Force releases Joint All-Domain Operations doctrine." https://www.aetc.af.mil/News/Article/2212411/air-force-releases-joint-all-domain-operations-doctrine/
5. Andreski, Nikolai and Adam Taliaferro. 2019. "Future Study Plan 2019 (Unified Quest) - Operationalizing Artificial Intelligence for Multi-Domain Operations." https://apps.dtic.mil/sti/trecms/pdf/AD1084346.pdf
6. Balboni, Mark, John A. Bonin, Robert Mundell, Doug Orsi, Craig Bondra, Antwan Dunmyer, Lafran "Fran" Marks, and Daniel Miller. 2020. "Mission Command of Multi-Domain Operations." Strategic Studies Institute, US Army War College, http://www.jstor.org/stable/resrep26552
7. Bott, Jonathan. 2017. "What's After Joint: Multi-Domain Operations as the Next Evolution in Warfare." https://apps.dtic.mil/sti/pdfs/AD1038879.pdf
8. Carlisle, Hawk. 2017. "The Complexity of Multi-Domain Operations." National Defense 102, no. 769. 4-5. https://www.jstor.org/stable/27022015.
9. Cordesman, Anthony A. and Grace Hwang. 2020." Chronology of Possible Russian Gray Area and Hybrid Warfare Operations." Center for Strategic and International Studies, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200702_Burke_Chair_Russian_Chronology.pdf
10. Fazekas, Ferenc. 2022. "A multitér (multi-domain) műveletek kialakulása és szükségessége." [The emergence and need for multi-domain operations] Hadtudomány 32. no. 2: 59-73. https://doi.org/10.17047/HADTUD.2022.32.2.59
11. Gompert, David C. 2003. "Preparing Military Forces for Integrated Operations in the Face of Uncertainty." RAND, Issue Paper https://www.rand.org/content/dam/rand/pubs/issue_papers/2005/IP250.pdf
12. Hegedűs, Ernő and Gyula Hennel. 2020. "Többdimenziós (multidomain) hadműveletek" [Multidomain Operations] Hadtudomány 30, no. 2: 3-27. http://doi.org/10.17047/HADTUD.2020.30.2.3
13. Jones, Marcus A. and Jose Diaz de Leon. 2020. "Multi-Domain Operations." The Three Sword Magazine 36, (November): 38–41. https://www.jwc.nato.int/application/files/5616/0523/5418/issue36_08lr.pdf
14. Lijphart, Arend. 1971. "Comparative Politics and the Comparative Method." American Political Science Review 65, no. 3: 682–693. https://doi.org/10.2307/1955513.
15. Mező, András. 2020. "Report on JAPCC Multi-Domain Conference." Hungarian Defence Review 148. no.1, 69-78. https://doi.org/10.35926/HDR.2020.1.6
16. Mező, András. 2021. "Multidomén műveletek vezetése és irányítása." [Command and control of multi-domain operations] Hadtudomány 31. no. 1, 3-21. https://doi.org/10.17047/HADTUD.2021.31.1.3
17. Mező, András. 2022. "Multidomén műveletek városi környezetben." [Multi-domain operations in urban environment] Hadtudomány 32. no. 2, 31-44. http://doi.org/10.17047/HADTUD.2022.32.2.31

18. NATO. 2014. “Wales Summit Declaration” Last modified July 04, 2022. NATO - Official text: Wales Summit Declaration issued by NATO Heads of State and Government (2014), 05-Sep.-2014
19. NATO Standardization Office, NATO Term https://nso.nato.int/natoterm/Web.mvc
20. Paikowsky, Deganit. 2021. “Why Russia Tested Its Anti-Satellite Weapon.” Foreign Policy. Last modified December 26, 2021. https://foreignpolicy.com/2021/12/26/putin-russia-tested-space-asat-satellite-weapon/
21. Pickvance, Christopher G. 2001. “Four varieties of comparative analysis.” Journal of Housing and the Built Environment 16, no. 1: 7-28. https://www.jstor.org/ stable/41107161
22. Ragin, Charles. 2014. The Comparative Method. Oakland: University of California Press.
23. Sartori, Giovanni. 1970. “Concept Misformation in Comparative Politics.” The American Political Science Review 64, no. 4: 1033-1053. https://doi.org/10.2307/1958356.
24. Schmid, Johann. 2020. “Hybrid Warfare – operating on multidomain Battlefields” https://c2coe.org/wp-content/uploads/Library%20Documents/Read-Ahead/20200904%20RA%20Seminar%202020%20Schmid.pdf
25. Stucl, Damjan. 2022. “Ruska Agresija na Ukrajino: Kibernetske Operacije” in Vpliv kibernetsega prostora na “moderno bojevanje”." Contemporary Military Challenges. Accessed June/July 4, 2022. https://www.researchgate.net/publication/361569176_RUSSIAN_AGGRESSION_ON_UKRAINE_CYBER_OPERATIONS_AND_THE_INFLUENCE_OF_CYBERSPACE_ON_MODERN_WARFARE
26. Townsend, Stephen. 2018. “Accelerating Multi-Domain Operations.” Military Review, 4-7. https://www.armyupress.army.mil/Portals/7/Army-Press-Online-Journal/ documents/Townsend.pdf
27. TRADOC. 2018. The U.S. Army in Multi-Domain Operations, 2028. Headquarters, United States Army, Training and Doctrine Command (Pamphlet 525-3-1). Accessed May 20. 2020. https://api.army.mil/e2/c/downloads/2021/02/26/b45372c1/20181206-tp525-3-1-the-us-army-in-mdo-2028-final.pdf
28. Vecsey, Mariann. 2021. “A Multidomén Integráció Lehetőségei és Kihívásai.” [Challenges and Opportunities of Multidomain Integration] Hadtudomány 31. no. 4, 27-38. http://doi.org/10.17047/HADTUD.2021.31.4.27
29. Wille, Dennis. 2019. “A Summary of Multi-Domain Operations.” New America. http://www.jstor.org/stable/resrep19977.5

1053477-3045-1396-24-28

MULTI-DOMAIN COMMAND AND CONTROL – AN ADAPTATION REQUIREMENT FOR THE ROMANIAN ARMED FORCES

George-Ion TOROI, PhD. candidate
Lieutenant colonel, PhD. candidate, senior instructor
„Carol I" National Defense University, Bucharest, Romania
E-mail: george_toroi@yahoo.com

Abstract*: In the dynamic landscape of contemporary warfare, characterized by the integration of multiple domains, the Romanian Army faces the imperative to evolve its command and control (C2) systems. This research paper explores the pressing need to adapt the Romanian Army's C2 framework to effectively operate in a multi-domain environment. The study analyses the challenges posed by the current character of warfare by examining the conceptual foundations of multi-domain operations (MDO). Furthermore, it explores the operational need for such an adaptation requirement, but also provides guidance on how to do this using a standard C2 framework.*
Keywords*: conflict, operating environment (OE), adaptation, command and control (C2), multi-domain, decision, operational domain*

Introduction

Since the beginning of time, armed conflicts have been part of human life. (Palazzo 2023, 9) The aphorism "*only the dead have seen the end of war*" often attributed to the ancient Greek philosopher Plato was, in fact, an expression used in a written form by American-Spanish philosopher George Santayana in his 1922 work, "*Soliloquies in England and Later Soliloquies*". (Braumoeller 2019, 5) This statement reflects the perpetual nature of conflict within human societies underscoring the cyclicality and the enduring presence of war as an intrinsic element of the human condition.

The conflicting nature of societies contributes to the significance of the military domain, as one of the key tools available to international actors alongside diplomatic, informational and economic instruments of power. (Doctrina Armatei României 2012, 13-14) (AJP-01 2022, 11-12) (JDP 0-01 2022, 12) (JP 1 2017, I-4) These four elements form a complete framework for nations to pursue their interests within the landscape of international relations. The importance of these instruments of power can vary based on the relationships between actors. Notably, during conflicts, the military one takes on a crucial role in implementing a state's strategy by utilizing force to achieve objectives. This instrument is essential for projecting power, safeguarding interests, and protecting a state's sovereignty from threats. The military's ability to operate across domains such as land, air, sea, space, and cyberspace is critical in modern conflicts, where multi-domain engagement is increasingly vital.

However, in today's complex environment, the effectiveness of the military in conflicts is not solely measured by its kinetic abilities—such as firepower, mobility, and force size—but also by its capacity to coordinate operations, with other national instruments of power (diplomatic, informational and economic) and to adapt to the changing character of warfare. This involves using technology, for intelligence gathering, surveillance, cyber activities, and precise engagement, while also maintaining readiness to counter asymmetric threats. It also includes the capacity to organize and effectively lead troops to achieve converging effects across all operational domains.

War encompasses both enduring elements as new ones. The theory of war categorizes these as the nature and character of conflicts. The distinction between these two is a fundamental concept in military theory, illustrating wars' dual facets that encompass both its constant core and its changing characteristics. On one hand, the **"*nature*" of war** pertains to the qualities of war that have persisted throughout history, regardless of circumstances or time periods. These aspects include the presence of violence and its destructive effects on societies, the constant friction, the clashes of wills, the fog of uncertainties arising from ambiguity, and elements of chance. The nature of war emphasizes that fundamentally war is an extension of politics by other means—a concept articulated by Carl von Clausewitz— involving a struggle for influence and power, and the imposition of one's will upon the adversary through the use of force.

On the other hand, the essence of warfare relates to the changing and unpredictable elements influenced by the evolving social, technological, economic, and political environments in which conflicts arise. This encompasses changes in the methods of warfare, the technologies and weapons employed, the strategies and tactics developed, and international laws that govern the conduct of war. They are all part of the **"*character*" of war.** It reflects the dynamic and evolving features of warfare, reflecting advancements in military technology, that subsequently impact how military operations are planned and executed.

Distinguishing between the nature and character of warfare holds great importance for military commanders and planners, policymakers, and academia as it aids in analyzing and preparing for conflicts. Acknowledging enduring aspects of war enables recognition of timeless principles applicable, across various conflicts. Simultaneously, acknowledging the evolving character of warfare demands **adaptation** and creativity to tackle challenges, leverage emerging opportunities, and counter risks posed by new technologies and geopolitical shifts.

However, the contemporary operating environment which is considered to be extremely complex (JCN1/17 2017, 1) (Future Leadership 2020, 1-2) (TC 7-102 2014, 1-2), generates additional pressure on military forces to identify adequate solutions to address current challenges. For this reason, a high degree of flexibility and adaptability is critical to succeed in operations. (Tim Sweijs 2020, 8) Adaptation has proven to be a vital element in times of war. (David Barno 2020, 11) (Ryan, Mick 2022, 131) Nevertheless, it is essential first to grasp a proper understanding of the operating environment (OE) and its features, in order to adopt proper adapting measures.

Nowadays the operational landscape is incredibly complex due to technological progress, the merging of traditional warfare domains with cyber and space as key battlegrounds, and the rise of asymmetric and hybrid warfare tactics. Globalization adds another layer of complexity by connecting economies and information systems, making conflicts no longer geographically isolated, which complicates planning military operations, considering the multitude of factors that can influence the outcome of the war. Moreover, the changing nature of threats, from tactics used by state and non-state actors to the pervasive issue of information warfare, requires a comprehensive defense approach, considering implications across all dimensions and domains. Consequently, military responses need to be adaptable, incorporating domains, utilizing advancements, and upholding ethical and legal standards against dynamic threats. This challenging environment calls for innovative strategies, international cooperation efforts, and continuous improvement of capabilities to effectively address modern geopolitical and security issues. Western nations have adjusted their approach to military operations in response, to these challenges.

The innovative approach known as **MDO (multi-domain operations)** combines the art and science of warfare (MCDP-1 2018, 1-17), blending practical knowledge, with creative military skills in diverse and challenging settings. Effective leadership and coordination of forces along with collaboration with other relevant actors within the area of responsibility are crucial for mission success in today's dynamic environment. The changing features of the environment have reshaped how Western militaries perceive command and control (C2). With the increasing likelihood of faceted conflicts, **C2 systems must evolve to confront these challenges** directly. As a result, a transition towards a **Multi-Domain Command and Control (MDC2)** approach has become imperative. MDC2 aims to improve the adaptability and integration of operations across all domains to ensure a flexible response to threats' complexity. This shift in C2 philosophy highlights the necessity for a framework that not only addresses traditional warfare elements but also includes cyber operations, information warfare, and strategic resource management across various domains. This approach optimizes actions effectiveness, within a global security landscape that is rapidly evolving. Many Western democracies have already begun adopting this approach to command and control.

Considering these developments, it seems that the Romanian approach to Command and Control (C2) may need some updates to keep up with operational needs. This serves as the **problem statement** for this research study. In this context, the adaptation of the Romanian C2 approach will facilitate a high degree of interoperability with allied nations and partners, which, consequently, will ensure effective collaboration in multinational operations. Therefore, I consider that addressing the modernization of Romania's Command and Control (C2) capabilities towards a Multi-Domain Command and Control (MDC2) framework is essential for aligning with NATO standards, enhancing effectiveness across all operational domains and adapting to new threats more effectively.

Research Methodology

The overall aim of this study was to highlight the importance of updating Romania's C2 systems to meet the evolving demands of warfare, especially emphasizing the shift, towards Multi Domain Command and Control (MDC2) capabilities.

This study specifically focuses on the Romanian Army aiming to offer solutions that are relevant at all levels of operations: strategic, operational, and tactical. The insights and recommendations put forth in this article, although primarily focused on the Romanian Armed Forces, have broader relevance and could be valuable to any military organization with some adjustments to fit specific circumstances.

In order to fulfill the aim of our study, this article addresses the following **research questions**:

1. Why C2 is crucial for mission success in the contemporary multi-domain environment?
2. What challenges does the current OE pose to the military C2 systems?
3. What factors should the Romanian Armed Forces consider when transitioning to Multi-Domain Command and Control (MDC2)?

This research analyses the Romanian C2 concept and suggests considerations that military leadership should take into account when adapting this concept to warfare evolution. Using an **exploratory and qualitative approach**, the study seeks to understand the importance and application of C2 systems in contemporary operating environments. It is structured as a **cross-sectional study**, focusing on examining current approaches to C2, while also providing insights, into future capabilities and developments. To enhance the study's main objective, a model known as PPST (People, Processes, Structures and Technologies) was employed to analyze C2 systems.

The PPST model is well known for its effectiveness in studying and examining the complexities of C2 systems, making it a suitable approach for this research. By utilizing the PPST model, the study aims to analyze the aspects of C2, offering an insight that can guide strategic decisions and operational methods to enhance the efficiency and flexibility of C2 systems in response to changing dynamics in warfare.

This article is divided into several key sections to achieve the stated aim of enhancing the understanding and adaptation of Command and Control (C2) systems within the Romanian Armed Forces, considering the evolving nature of warfare. Initially, it discusses the significance of C2 for mission outcomes, highlighting its substantial benefits for military forces during conflicts.

Furthermore, it tackles the challenges presented by today's operating environment (OE) to C2 systems, stressing the need for these systems to evolve. The dynamic and complex nature of modern warfare, characterized by technological advancements and the blurring of traditional warfare domains, necessitates adaptable, robust C2 systems, capable of integrating operations across various domains.

The final section offers an in-depth evaluation of C2 systems through the framework of PPST (People, Processes, Structures and Technologies). Based on this comprehensive examination, the article provides suggestions, for the Romanian Armed Forces to help streamline the adjustment of its C2 systems. These recommendations are aimed at enhancing mission success in an evolving global security landscape.

Command and control – critical warfighting function for mission success

In war, no single activity is more important than command and control. (MCDP-6 2018, 1-3) C2 serves as the element that brings together and gives structure to all functions and activities. It acts as the foundation of prowess by establishing the framework and procedures through which decisions are formulated, communicated, and carried out across the entire spectrum of military activities. C2 guarantees that military endeavors such as logistical support, intelligence gathering, or tactical maneuvers are not isolated actions, but are coordinated and aligned with overarching goals and objectives of military operations.

Without C2, these individual functions would lack guidance and purpose functioning independently rather than as integral parts of a unified effort. C2 plays the role of converting individual actions into a collective endeavor, by ensuring each function contributes meaningfully to mission success. It harmonizes the diverse elements of military operations – from planning to execution to evaluation –, into a cohesive whole, thereby maximizing the synergistic effects of all military capabilities. Understanding C2 as the central mechanism through which command is exercised and all military operations are controlled and coordinated, is essential for achieving operational effectiveness.

Command and control, which involves the exercise of authority by designated commanders over assigned forces, is an essential element in both warfare's art and science. (FM 6-0 2022, 1-1) It highlights commanders' pivotal role in coordinating all aspects of operations. C2 serves as more than another function within the military; it is the structure that provides purpose and coherence to all other functions. Through C2, commanders provide direction to their forces, integrating military activities into a cohesive effort aimed at achieving mission success.

In essence, C2 is the mechanism by which military operations are planned, managed, and carried out, playing a decisive role in attaining objectives and mission achievements. Without efficient C2 practices, military operations would lack the coordinated effort needed to address the challenges of warfare effectively. Commanders, through their exercise of C2, ensure that every aspect of military power is harmonized towards a shared objective, highlighting the critical importance of C2 in the orchestration of military endeavors.

To implement effective command and control (C2) practices, it is crucial to have a grasp of its fundamental essence. This involves understanding its purpose, characteristics, operational environment, and basic functions. The main goal of C2 is to equip leaders with the ability to exert authority and guidance over assigned and attached forces in achieving the mission. Its key traits include flexibility, resilience, responsiveness, and the coordination of actions, across domains and command levels. The operational landscape where C2 functions is becoming more intricate due to rapid technological advancements, multi-domain battlefields, and unconventional threats that require agile and adaptive responses.

Effective Command and Control (C2) plays a critical role in harmonizing the conceptual, physical, and moral components of fighting power, thereby enhancing the overall effectiveness of military operations. By establishing clear goals, facilitating effective communication channels, and optimizing resource allocation processes, C2 reinforces the conceptual component through well-informed decision-making strategies and innovative approaches. It enhances the physical dimension by ensuring the deployment of personnel, armaments, and logistical support for maximum operational effectiveness. Moreover, C2 strengthens the moral aspect by promoting unity among troops, through fostering confidence and ethical behavior for maintaining high morale levels, essential for sustained combat readiness.

This integrated approach not only consolidates the various elements of fighting power but also ensures that they are effectively employed in a coordinated manner to achieve mission success, demonstrating the decisive role of robust C2 systems in contemporary military operations.

C2 plays a key role in operations by providing a comprehensive ability to sense and understand the operational environment, anticipate future conditions, and efficiently communicate, guide, manage, and decide on the best courses of action. It allows forces to act decisively, influence outcomes, coordinate with allied forces, manage information across levels, and plan subsequent steps. C2 forms the foundation for the unity of effort and effective decision-making processes that enable adaptation to evolving situations, risk management, and optimal resource allocation. By driving the operations process, C2 ensures that all aspects within an operation are harmoniously influenced and directed to enhance efficiency and achieve objectives in today’s complex and dynamic environment.

Current operating environment challenges to C2 systems

However, today, more than ever, the ability to decide better and quicker than your adversary is paramount. “*Decision dominance is aspirational, situationally dependent, and always relative to an opponent. The goal is to understand, decide, and act faster and more effectively than the threat.*” (FM3-0 2022, 3-14) This concept highlights the necessity for adaptable command and control (C2) systems that can overcome contemporary operational threats.

Nonetheless, the contemporary operating environment poses an array of challenges to Command and Control (C2) systems, each requiring specific attention to ensure operational effectiveness in military operations. This section outlines some of the key challenges that C2 systems must address.

To start with, in the age of **information warfare**, the sheer amount and speed of data generated pose a significant challenge to C2 systems. These systems must quickly process and filter this data to provide relevant intelligence. Information overload is considered one of the main issues that C2 systems must confront. (James Black 2024, 23) The challenge intensifies with the need to differentiate between credible information and potential misinformation or disinformation campaigns. The use of information to confuse, mislead, or influence the decision-making processes of adversaries has become a central aspect of modern conflicts. C2 systems must navigate an environment saturated with both accurate and deceptive information, requiring advanced analytical capabilities to differentiate reality from manipulation. In this respect, effective C2 systems must incorporate advanced data processing technologies, such as real-time analytics and big data processing capabilities, to handle this challenge

Modern conflicts are characterized by increased **complexity**, with **operations** spanning **across multiple environments** and involving a wide range of actors, both state and non-state. This complexity reduces the control that militaries have over the situation. To navigate this uncertainty, C2 systems must provide a comprehensive understanding of not just the physical battleground, but also the socio-political and cultural factors at play. This requires tools that can gather and analyze data from a variety of sources to create a comprehensive intelligence picture. That will enable effective decision-making.

The increased **volatility** of the operational situation in the current environment makes it critical for armed forces not only to make appropriate decisions but also to be able to do it extremely fast. In this respect, modern C2 systems are challenged to deliver a faster OODA (Observe, Orient, Decide, Act) loop. This demands system designs that enable information processing, efficient decision-making frameworks, and streamlined command structures. While emerging technologies, such as artificial intelligence, can improve this process, there are concerns about maintaining a balance between machine-driven decisions and human-centered approaches. Nevertheless, today's world trend is to incorporate technology as much as possible to enhance the speed and accuracy of decision-making processes.

However, converting decisions into coordinated actions on the battlefield is not that easy. Command and control (C2) systems must facilitate concise communication of orders, seamlessly integrating them into various military units' operations. This necessitates communication systems that can function across military branches and with allied forces, ensuring synchronized and effective execution of orders.

Decision dominance has always been a prerequisite for operational success. This involves maintaining a faster and better OODA (observe orient, decide, act) loop than your adversary. Decision dominance refers to *the ability of the commander to sense, understand, decide, act, and assess faster and more effectively than any adversary."* (Tunnell September-October 2022, 79) In the context of Command and Control (C2) systems, this means developing and maintaining capabilities that can efficiently navigate through each phase of the OODA loop, thereby ensuring superior decision-making and operational tempo. Figure no. 1 depicts specifics on how to obtain decision dominance in modern confrontations.

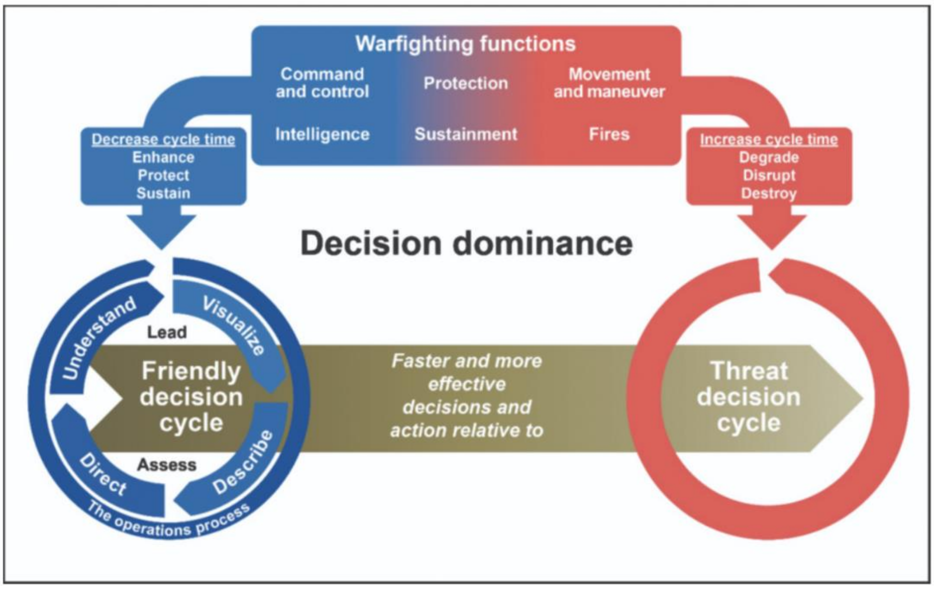
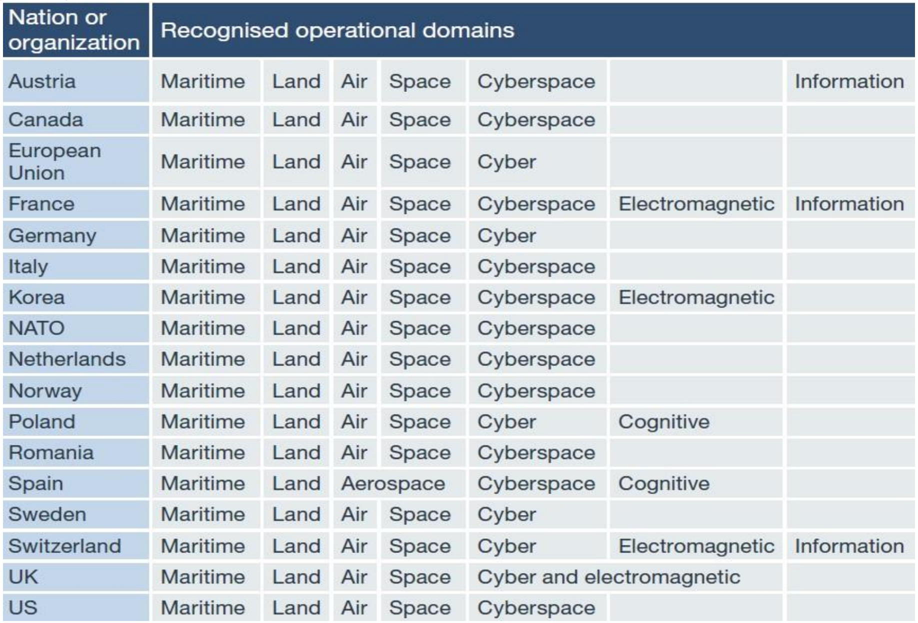


Figure no. 1. Decision dominance (Maj. Christopher Kean November-December 2022, 111)

Furthermore, C2 systems must provide proper guidance and coordination in response to evolving situations. Considering that unpredictability is one key characteristic of warfare, this is not an easy task. To effectively respond to emerging threats, changes in the operating environment, and evolving enemy tactics, it's crucial to have flexible C2 systems. These systems should be able to integrate new technologies, methodologies, and strategies while also adjusting processes and structures as required. In modern warfare, it is recognized that *„the force that orientates, innovates and adapts more quickly than their adversary in conflict is likely to gain an advantage and achieve their objectives."* (AJP-01 2022, 73)

The rapid evolution of technological change presents both opportunities and challenges for C2 systems. Keeping up with and incorporating advancements like AI, cyber capabilities and unmanned systems is vital to maintain a functional C2. However, this continuous technological evolution demands sustained investment, rigorous testing, and training, and the development of new doctrines and operational concepts. These all aspects are critical for developing adequate C2 systems.

Furthermore, **operations in modern warfare are not confined to a single domain** but extend across multiple domains. The concept of "domain" in military terms refers to a distinct sphere of operations where a specific set of activities are undertaken to achieve defined objectives. (Multi-Domain Multinational Understanding 2022, 12) This definition encompasses not only the traditional physical domains of land, air, and sea but also extends to newer realms such as space and cyberspace. Each domain has its unique characteristics that influence how operations are planned and executed within it. However, there isn't an agreement, on these domains with each country recognizing its specific areas. Figure no. 2 depicts the domains acknowledged by different nations.



Nation or organization	Recognised operational domains						
Austria	Maritime	Land	Air	Space	Cyberspace		Information
Canada	Maritime	Land	Air	Space	Cyberspace		
European Union	Maritime	Land	Air	Space	Cyber		
France	Maritime	Land	Air	Space	Cyberspace	Electromagnetic	Information
Germany	Maritime	Land	Air	Space	Cyber		
Italy	Maritime	Land	Air	Space	Cyberspace		
Korea	Maritime	Land	Air	Space	Cyberspace	Electromagnetic	
NATO	Maritime	Land	Air	Space	Cyberspace		
Netherlands	Maritime	Land	Air	Space	Cyberspace		
Norway	Maritime	Land	Air	Space	Cyberspace		
Poland	Maritime	Land	Air	Space	Cyber	Cognitive	
Romania	Maritime	Land	Air	Space	Cyberspace		
Spain	Maritime	Land	Aerospace		Cyberspace	Cognitive	
Sweden	Maritime	Land	Air	Space	Cyber		
Switzerland	Maritime	Land	Air	Space	Cyber	Electromagnetic	Information
UK	Maritime	Land	Air	Space	Cyber and electromagnetic		
US	Maritime	Land	Air	Space	Cyberspace		

Figure no. 2. Operational domains (Multi-Domain Multinational Understanding 2022, 12)

The challenge for C2 systems lies in coordinating activities across these recognized domains to ensure operational synergy. This requires not only technological solutions for cross-domain communication, but also doctrinal and procedural frameworks that facilitate multi-domain operations. Considering the various challenges presented by the current operating environment, many NATO nations and NATO itself are increasingly adopting a **multi-domain operations (MDO) approach**. This shift is driven by the need to effectively address the complexities and changing nature of contemporary warfare. NATO views MDO as the ***„orchestration** of **military activities**, across all domains and environments, **synchronized** with*

***non-military activities**, to enable the Alliance to create **converging effects** at the speed of relevance*". (Alliance Concept for Multi-domain Operations 2023, 9)

Furthermore, NATO emphasizes the importance of the **cognitive domain** in future engagements. (Guyader 2022, 3-1) The 2021 commitment made by Allied Heads of State and Government to implement the NATO Warfighting Capstone Concept, signifies an acknowledgment of the evolving character of modern warfare. One of the imperatives is related to the concept of superiority in all operational domains, particularly emphasizing cognitive superiority, which is seen as vital for NATO operations. (NATO WARFIGHTING CAPSTONE CONCEPT 2021, 10) It refers to the capacity to outsmart opponents, in understanding and decision-making, thus enabling NATO forces to out-think and out-maneuver opponents. Achieving cognitive superiority involves developing a faster, deeper, and broader understanding of the operating environment, adversaries, and self-awareness, coupled with superior decision-making capabilities. This generates a necessity for C2 systems to evolve and adapt to fulfill these operational requirements „*across all physical and non-physical domains*". (NATO WARFIGHTING CAPSTONE CONCEPT 2021, 17)

Moreover, in an era where coalition operations are the norm, **interoperability** becomes a critical aspect of C2 systems. These systems must possess the ability for communication and coordination with allied forces that may utilize equipment and follow diverse operational doctrines. Establishing standards, protocols, and systems that can function effectively within a coalition setting poses a challenge for military C2 systems. This applies to NATO forces as well and is a huge challenge the Alliance needs to address.

To sum up, the obstacles encountered by C2 systems are multidimensional, necessitating a combination of technological advancement, doctrinal creativity, and continuous adaptability. Confronting these challenges is essential for ensuring operational effectiveness and success within the realm of contemporary warfare. In this respect, Multi-Domain Command and Control (MDC2) represents an evolved approach to C2, designed to integrate operations across all operational domains and address these challenges.

Developing a Multi-Domain Command and Control Framework for the Romanian Armed Forces – why and how

For the Romanian Armed Forces, adapting to the changing dynamics of warfare is imperative. This adaptation involves embracing Multi-Domain Operations (MDO) and integrating them into operational doctrines for seamless interoperability within NATO. This includes revising training programs to include MDO concepts, participating in joint exercises with NATO allies, and fostering a culture of innovation and adaptability within the armed forces. Despite some academic discussions in Romania regarding the adoption of Multi-Domain Operations, the progress made is modest when compared to NATO allies who have made strides in incorporating MDO into their operational frameworks.

Furthermore, Romania faces challenges from a Command and Control (C2) perspective due to its hesitation in embracing Multi-Domain Operations (MDO). Robust C2 systems are the backbone of any military operation, requiring advanced communication, data sharing, and decision-making processes that transcend traditional domain boundaries. Without aligning its C2 structures with MDO principles, Romania risks falling in areas such, as real-time data fusion, cross-domain situational awareness, and agile decision-making capabilities. This misalignment could lead to delays in command response, inefficiencies in resource allocation, and decreased operational tempo, ultimately impacting mission success in a multi-domain environment. To address these issues, Romania would need to enhance its C2 systems to handle the complexity of MDO. This involves upgrading technological infrastructure, developing new operational doctrines, and training personnel in multi-domain strategies. Such advancements would not only boost Romania's operational effectiveness within NATO but also ensure that its forces are ready to counter the diverse threats of modern warfare.

A practical approach for the Romanian Armed Forces in adapting its C2 system to contemporary operational demands is to apply the People, Processes, Structures, and Technologies (PPST) framework. This comprehensive model offers a holistic perspective on Command and Control (C2) capabilities and the challenges they face. This systematic approach will assist the Romanian Armed Forces in establishing a flexible and integrated command and control system, that aligns with NATO standards and contemporary warfare demands.

When evaluating a Command and Control (C2) system for the Romanian Armed Forces using the PPST framework, it is crucial to consider the following key elements to ensure that any changes align with operational objectives and enhance overall military effectiveness.

- *Effectiveness*. This pertains to whether the C2 system is contributing to higher-level military objectives. It involves assessing how well the system supports the overall mission success. For example, an effective C2 system would enhance decision-making, improve response times, and ensure accurate and timely information flow, all pivotal in achieving goals.
- *Efficacy*. This criterion examines whether the C2 system is delivering desired outcomes. It focuses on output quality and meeting system goals. For a C2 system, efficacy could be measured in terms of accurate situational awareness, the precision of command execution, and the ability to adapt to changing operational environments. Essentially, it's about how effectively the system fulfills its intended role, in real-world situations.
- *Efficiency*. This aspect centers on how resources are utilized within the C2 system. It examines whether the system is using the minimum resources necessary to achieve its goals. This encompasses making use of human resources, technology, time, and information An efficient C2 system would operate with minimal waste, lower costs, and higher productivity, maximizing the value of resources invested in it.

The following serves as a set of recommendations for the Romanian Armed Forces in order to adapt to MDC2. It employs the **PPST framework** previously mentioned.

People

The human factor is fundamental in a Command and Control (C2) system. Recognizing and dealing with the capabilities and limitations of human nature is essential for developing and operating a successful C2 system.

The effectiveness of MDC2 depends on the abilities, training, and cognitive adaptability of its personnel. This involves cultivating leaders and operators who can think and operate across domains, understanding how actions in one domain affect others. Developing such expertise requires specialized, multidisciplinary training that focus on joint operations, decision-making amidst uncertainty, and utilizing intelligence from diverse sources. Furthermore, promoting a culture of innovation and flexibility among personnel is crucial for the setting of MDC2.

When examining Multi-Domain Command and Control (MDC2) from a "*People*" perspective it is crucial to delve into human resource development, the approach of mission command, and the impact of human factors on improving MDC2 capabilities. Each of these elements plays an important role in ensuring that MDC2 is not only technologically advanced but also effectively led, managed, and carried out by highly skilled individuals.

Recognizing and addressing human cognitive limitations, stress, and decision fatigue is also vital. Command and control systems should be designed to support decision-makers, not overwhelm them. Additionally developing human strengths such as intuition, adaptability, creativity, teamwork, and communication is essential. The Romanian Armed Forces must find solutions to foster these abilities for an MDC2 system that can drive operations towards success on the battlefield. Moreover, cultivating leaders and operators who can seamlessly integrate with technologies while functioning effectively in technology-limited environments is crucial for the success of MDC2 in contemporary and future conflicts. Furthermore, involving civilian experts can provide knowledge in critical areas like cybersecurity and artificial intelligence that are indispensable in modern warfare.

Processes

The development of processes that facilitate planning, decision-making, and execution across domains becomes imperative for MDC2. The integration of intelligence, surveillance, and reconnaissance (ISR) efforts, along with coordinating kinetic and non-kinetic effects, and establishing communication protocols for secure information exchange are key components. Additionally, processes should involve risk assessment and management strategies that consider the complexities and interdependencies of multi-domain operations.

Examining Multi-Domain Command and Control (MDC2) from the perspective of procedures, capability growth, and alignment processes reveals the structure needed for successful multi-domain operations. To effectively adapt the Romanian approach to Multi-Domain Command and Control (MDC2), several critical process adjustments and improvements are required. These changes aim to establish an agile and technologically advanced C2 system capable of operating effectively across multiple domains and in coalition environments. For this reason, when considering adapting the „Processes" component of a C2 system, the following should represent key areas of focus:

- enhancing Common Operational Picture (COP) and Common Intelligence Picture (CIP);
- synchronizing Battle Rhythm adjustments;
- incorporating technology to enhance operational efficiency, increase accuracy and quickly share critical information with relevant stakeholders, at multiple levels;
- adopting a systems approach to process design as depicted in Figure No. 3;
- continuous process improvement and alignment with NATO and partners' MDC2 approach.

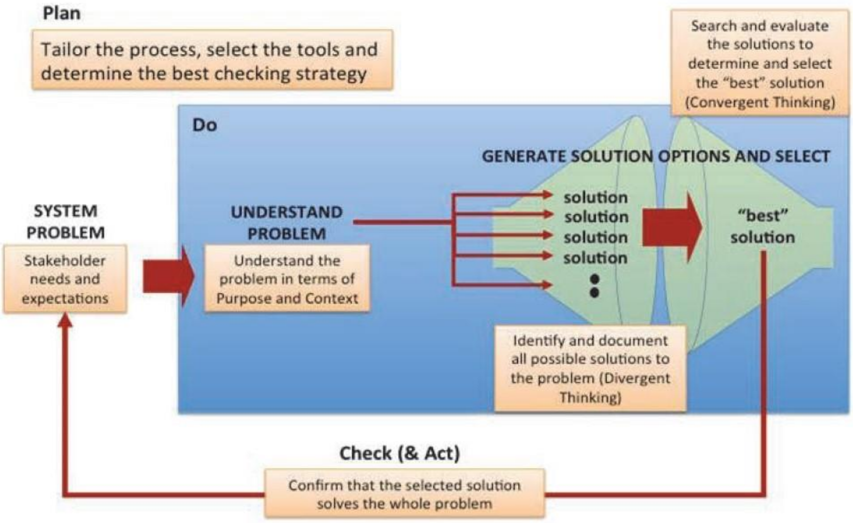

Plan
Tailor the process, select the tools and determine the best checking strategy
Search and evaluate the solutions to determine and select the "best" solution (Convergent Thinking)
Do
GENERATE SOLUTION OPTIONS AND SELECT
SYSTEM PROBLEM
Stakeholder needs and expectations
UNDERSTAND PROBLEM
Understand the problem in terms of Purpose and Context
solution
solution
solution
solution
"best" solution
Identify and document all possible solutions to the problem (Divergent Thinking)
Check (& Act)
Confirm that the selected solution solves the whole problem

Figure no. 3. A systems approach to command and control (James Black 2024, 121)

Structures

The organizational structures that support MDC2 must facilitate unity of command and interoperability across all operational domains and dimensions. In this respect, the Romanian

Armed Forces should consider making some structural changes to ensure proper management and coordination of military operations in a more and more complex environment.

To start with, establishing **Integrated Command Centers** is of crucial importance. These centers should oversee operations across all domains simultaneously, ensuring a unified approach to multi-domain operations. Centralizing command and control functions will lead to increased speed and accuracy of the decision-making process.

Additionally, developing flexible C2 structures is also a factor to consider for mission success. In today's warfare things are always changing, making it important to have C2 structures that can adapt quickly and be able to direct the operations towards the desired end-state. This flexibility is crucial for responding to emerging threats and diverse tactical situations, ensuring operational agility.

Another important aspect is having **unity of command** within these integrated centers. A defined hierarchy is essential for making adequate decisions and carrying out operations across multiple domains. This would enhance clarity, reduce confusion, and ensure that orders are efficiently communicated and executed. When it comes to Multi-Domain Operations (MDO), the Romanian Armed Forces are faced with critical decisions regarding the organizational structures. It should decide whether the traditional J-structure is applicable and efficient in this type of operation or it needs changing to be able to integrate actions and create synchronized effects across several operational domains. However, one should consider that a sudden change might create more chaos in the near future, this needing a lot of time to be properly understood within the force and trained accordingly. A near-term optimal solution might be an adjustment of the J-structure as it relies on a decades-old solution that is deeply rooted within the armed forces.

Moreover, a thorough analysis of the CP (Command Post) structure should be regarded. Learning from the experiences in the ongoing conflict in Ukraine, it's vital to consider the concept of **Command Post (CP) dispersion.** This concept plays an important role in strengthening command structures in today's operational settings, ensuring the protection and functionality of C2 regardless of the transparency of the current battlefield, where potential enemies can more easily detect and engage C2 physical structures. Another solution might impose choosing a different setting for the CP, outside the engagement possibilities of the enemy. However, in this situation **reliance on technology is paramount** in order to communicate orders and direct subordinate forces.

In an era where threats can emerge from multiple domains simultaneously, having a viable command post structure helps reduce vulnerability and ensures operational readiness, in different situations. This emphasizes the importance of finding adequate and innovative solutions for CP protection, as previously mentioned.

Furthermore, it is crucial for the Romanian Armed Forces to prioritize organizing their command and control (C2) systems to facilitate efficient information management and maintain a consistent battle rhythm. This involves setting up protocols for accurate information processing ensuring that decision makers have access to real-time data for effective responses to evolving circumstances.

In addition, **a strong focus on interoperability** is essential, particularly considering Romania's position within NATO. Considering the high possibility of operating in a multinational environment, Romanian C2 structures should be designed to promote coordination and communication across domains as well as with international allies. As such, a high level of interoperability would facilitate Romania to operate in joint multinational multi-domain operations.

Lastly, these structural adjustments should be **tailored** for a range of scenarios spanning across the full spectrum of a continuum of competition. The established structures should enable the Romanian Armed Forces to transition smoothly across the spectrum of cooperation, rivalry, confrontation, and armed conflict. (AJP-01 2022, 5 - 7)

Technology

The technological foundation of MDC2 encompasses a range of systems and platforms that enhance situational awareness and understanding, communication capabilities, and effective operations direction and coordination across different operational domains.

Command and Control (C2) systems play a critical role, in today's operating environment by providing a comprehensive operational picture that enables quick decision-making and coordinating actions effectively. The use of technology in MDC2 systems improves awareness, decision accuracy, and the ability to exert influence across domains simultaneously. This makes it a decisive component of an effective MDC2 system. However, considering the growing importance of the **cyber domain and the inherent threats** that come with it, proper **MDC2 protection measures** should be considered. Moreover, the **redundancy of technical assets** should also be considered.

Enhancing Romania's Multi-Domain Command and Control (MDC2) capabilities involves **acquiring cutting-edge technologies** like satellite communications, cyber defense systems, unmanned platforms, and advanced sensors. These technologies enhance domain awareness, ensure communication across different operational domains, and facilitate all functions of a C2 system in the modern conflict.

Moving towards a **data-centric operational and technological approach** is essential for Romania. This shift should include the modernization of existing systems to align with the needs of multi-domain operations. A data-centric approach facilitates better decision-making and resource allocation, ultimately improving efficiency.

However, considering the high possibility of operating in a multinational environment, the success of Romania's MDC2 strategy hinges on ensuring **interoperability** with NATO allies' technological systems. Maintaining interoperability along with cybersecurity measures is crucial for safeguarding these systems against evolving cyber threats. Protective measures play an essential role in today's warfare landscape ensuring integrity and effectiveness. Harmonizing systems with NATO allies is key for successful multinational multi-domain operations (M2DO), enhancing strategic partnerships. Operating effectively within NATO structures is vital for Romania's defense efforts. For this crucial reason, technical interoperability should be a top priority when considering adopting an MDC2 system.

Conclusions

In conclusion, this study has thoroughly examined the importance of modernizing the Romanian Armed Forces Command and Control (C2) systems to adapt to the complexities of modern warfare. The shift towards Multi-Domain Command and Control (MDC2) system is not a choice, but a necessity in the ever-evolving operating environment.

This research emphasized the indispensable role of C2 in achieving mission success across operational domains. An effective command and control system serves as the core framework for coordination, decision-making, and execution across domains, crucial for Romania's integration into NATO C2 systems and for addressing global security challenges. The contemporary operating environment, characterized by technological advancements, increased complexity, and convergence of traditional warfare realms presents significant challenges for existing C2 structures. The Romanian Armed Forces must address these challenges by using a strategy outlined in the People, Processes, Structures and Technologies (PPST) framework. This method is crucial for a unified approach to the complexities of modern warfare. This comprehensive approach ensures a robust, agile, and resilient military force capable of facing the diverse challenges posed by the contemporary operational landscape.

In summary, this article not only highlights the urgent need for transformation in the C2 systems of the Romanian Armed Forces but also provides a roadmap for ongoing development towards this end in the face of evolving global security challenges.

BIBLIOGRAPHY:

1. AJP-01. 2022. *AJP-01, Allied Joint Doctrine, Edition F, Version 1.* NATO Standardization Office.
2. 2023. *Alliance Concept for Multi-domain Operations.* NATO.
3. Braumoeller, Bear F. 2019. *Only the dead: the persistence of war in the modern age.* Oxford: Oxford University Press.
4. David Barno, Nora Bensahel. 2020. *Adaptation under Fire. How Militaries Change in Wartime.* Oxford University Press.
5. *Doctrina Armatei României.* 2012. București. Statul Major General.
6. FM 6-0. 2022. *FM 6-0 Commander and Staff Organisation and Operations.* US Department of the Army.
7. FM3-0. 2022. *FM 3-0 Operations.* Washington: US Department of the Army.
8. *Future Leadership.* 2020. Multinational Capability Development Campaign.
9. Guyader, Hervé Le. 2022. "Cognitive domain: A sixth domain of operations." In *Cognitive Warfare: The Future of Cognitive Dominance*. NATO Science and Technology Organization.
10. James Black, Rebecca Lucas, John Kennedy, Megan Hughes, Harper Fine. 2024. *Command and control inthe future. Concept paper 1: Grappling with complexity.* Santa Monica, California: RAND Corporation.
11. JCN1/17. 2017. *Joint Concept Note (JCN) 1/17 – Future Force Concept.* UK Ministry of Defence.
12. JDP 0-01. 2022. *Joint Doctrine Publication 0-01 UK Defence Doctrine, ediția a șasea.* UK Ministry of Defence.
13. JP 1. 2017. *Joint Publication 1 Doctrine for the Armed Forces of the United States.* US Joint Chiefs of Staff.
14. Maj. Christopher Kean. November-December 2022. "Conceptualizing Information Advantage using Boyd's OODA Loop." *Military Review* 109 - 115.
15. MCDP-1. 2018. *MCDP 1, Warfighting.* US Marine Corps.
16. MCDP-6. 2018. *Command and Control.* US Marines Corps.
17. *Multi-Domain Multinational Understanding.* 2022. Multinational Capability development Campaign.
18. *NATO WARFIGHTING CAPSTONE CONCEPT.* 2021. NATO Allied Command Transformation.
19. Palazzo, Dr Albert. 2023. *Land Warfare: An Introduction for Soldiers, Sailors, Aviators and Defence Civilians.* Australian Army Occasional Paper No. 14, Australian Army Research Centre.
20. Ryan, Mick. 2022. *War Transformed. The Future of Twenty-First-Century Great Power Competition and Conflict.* Annapolis, Maryland: US Naval Institute Press.
21. TC 7-102. 2014. *Training Circular No. 7-102 Operational Environment and Army learning.* Washington DC: Headquarters Department of the Army.
22. Tim Sweijs, Frans Osinga, Samuel Zilincik, Martijn Vorm, Ivor Wiltenburg, Bianca Torossian. 2020. *The NATO Warfighting Capstone Concept: Key Insights from the Global Expert Symposium Summer.* Hague: The Hague Centre for Strategic Studies.

23. Tunnell, Col. Harry D. September-October 2022. "Command Post Automation." *MILITARY REVIEW* 79-86.

1053477-3045-1396-24-29

MILITARY MOBILITY IN EUROPE, A BRIDGE FOR NORTH ATLANTIC TREATY ORGANIZATION (NATO) – EUROPEAN UNION (EU) COOPERATION

Cătălina Ionela MANOLACHE, PhD. candidate
PhD. candidate, ”Carol I” National Defence University, Bucharest, Romania
E-mail: catalinagrigore2694@gmail.com

Aurelian Eusebio MANOLACHE
Major, Headquarters Multinational Division South-East, Bucharest, Romania
E-mail: mardare92@gmail.com

***Abstract**: Russia's invasion of Ukraine and its long-term effects on European security have led to a closer relationship between the EU and NATO. Military mobility is a „flagship" of the EU-NATO cooperation, serving as an instrument for the continuation of the projects regarding the Transatlantic defence. This article examines the main areas that can improve the partnership between the two security organizations, with a focus on the military mobility project.*

***Keywords:** military mobility, cooperation, partnership, NATO, EU,*

Introduction

Opinions urging the development of cooperation between NATO and the EU are expressed at high level. Even Josep Borell, vice-president of the European Commission, stated, in 2022, that „*working together: a stronger and more capable European defence also strengthens NATO. EU-NATO cooperation is crucial for European, transatlantic and global security. Making this cooperation even deeper will remain at the heart of the EU's defence efforts".* All these statements of the leaders of the two organizations highlight the fact that the changes in the security environment of the Europe have become an essential factor for the of the strengthening of NATO-EU relationship. Complex security challenges require closer cooperation, as neither one of the two organization can fully deal with military and non-military security threats. EU and NATO security plans are interconnected. By working together in order to achieve their objectives, they can make better use of the resources and instruments available to face the challenges and increase the security of their citizens.

In a volatile and unstable environment, cooperation between the EU and NATO is essential for the development of future security projects. The two organizations are linked not only through 22 member states of both the EU and NATO, but also by the ability to mobilize, through joint projects, a wide range of instruments which contribute to the achievement of the objectives at the highest level.

Russia's large-scale invasion of Ukraine has made military mobility a priority for common security and a way to increase the cooperation between the two structures. Bringing to the fore of traditional military threats and the increased attention on territorial defence contribute to highlighting the need to remove obstacles that could prevent military forces from moving quickly within the European space. Currently, both NATO and the EU need to improve their military mobility, as personnel and military equipment are moved to the eastern flank by NATO, which has constantly strengthened this area. On the other hand, the EU is using the infrastructure because it sent significant amounts of equipment to Ukraine, so that the country resist and remove the Russian threat. In order for all these actions to take place, the EU and NATO are planning detailed missions and put together their efforts to make deployment of forces as efficient as possible. Even though the military mobility project is still at an early stage, both organizations seem willing to make constant and joint efforts to achieve good results.

On the other hand, relations between NATO and the EU have not always been simple. Political tensions between some member states have sparked misunderstandings, particularly when it comes to information sharing. In front of all these global changes, NATO and the EU have revealed differences in leadership, culture and objectives. Still, the military mobility project seems to come as a hope that better collaboration can take place.

Through this paper, we intend to highlight the fact that military mobility is a project that seems promising in terms of improving cooperation between NATO and the EU, and based on what has been reported, make recommendations and predictions about how this cooperation could evolve. Given the predominantly military nature of both organizations, we believe that NATO and the EU can easily reach the use of a common language, which would allow the creation of a strong bond, in which each organization would come with its individual capabilities: the EU could rely on NATO's logistics expertise to strengthen its own military posture, while NATO could rely on EU's expertise in countering disinformation and improving military mobility.

In the first part, this paper examines the main issues that limit or prevent full engagement in a successful partnership by NATO and the EU. Afterwards, it broadly describes the evolution and current state of the cooperation between the two structures. In the last part, it highlights the connector role of military mobility and how cooperation between the two organizations has increased through joint projects in the field of movement and transportation (Giovanna De Maio, 2021).

Chapter 1: Main dissensions between NATO and the EU

There are several areas that cause problems in the relationship between the two organizations. One of them is the limited number of communication channels. Although progress has been made in terms of communication, the lack of a secure communication system significantly reduces their ability to work together, but most importantly: it poses coordination problems in the event of a real crisis. Also, the problems are related to different strategic priorities and political tensions. For example, Turkey's purchase of S-400 surface-to-air missiles from Russia and its invasion of northern Syria after United States (US) troops withdrew raised the concern of the allied states (Crisis Group, 2021). Nor are France's relations with Great Britain any better since the AUKUS deal, which also impact the functioning of NATO. These are just a few examples, but the differences between NATO and the EU do not stop here. While NATO is rethinking its military commitments and reflects on its capacity building and addresses diplomatic gaps, the EU is focusing on improving its military power (Giovanna De Maio, 2021).

Within NATO-EU relations, some states have more responsibilities than others, and the position of the more important actors determines the general framework in which states align more towards NATO or more towards the EU. The interminable conflict between Cyprus and Turkey is one of the reasons that have hampered progress in practical cooperation between the two organizations. Even today, this situation hinders the exchange of intelligence. Turkey has developed a pattern of objecting to NATO's decisions and leans more towards EU's policy, while Greece and Cyprus are reluctant when it comes to Turkey's involvement in EU projects, which has complicated and delayed agreements on Common Security and Defense Policy (CSDP) initiatives, leading to restrictive rules for association with non-EU members.

The situation seems to remain this way, given the fact that NATO cannot or does not want to take measures against a Turkey that sometimes has contrary attitudes to the other allied, as is the case of the blackmail regarding receiving the status of member of the organization by Finland and Sweden. Also, Great Britain's position towards NATO and the EU is causing dissension and directs other states to follow its path. The state seems to be more NATO-oriented and more skeptical about the EU, which is why it chose to leave the organization (Droin, 2023).

A key element is the institutional challenge that NATO and the EU are facing and the difference in missions and priorities of each. While NATO focuses on defense and deterrence and emphasizes the role of military logistics and sustainment in the European space, the EU focuses on crisis management, commercial rules, regulations and infrastructure development. However, because of these differences, NATO and the EU are, somehow, forced to common responsibility of establishing the necessary conditions for the movement of forces in Europe. The member states of both organizations must consider military mobility as part of their national political processes and at the same time balance the competitive priorities of each participating organization (Hans-Werner Wiermann, 2023).

Although military mobility situation between the EU and NATO is not completely clarified and the cooperation still presents some gaps, the efforts made to solve them and to produce the desired effects in the field are very great on both sides. For example, through the Structured Dialogue and the PESCO military mobility project, the aim is to fill in the lack of a formal structure to ensure the exchange of information through informal, time-consuming means that can send a wrong message. A concern regarding cooperation in the field of military mobility between NATO and the EU is the different way of classifying information by the two institutions. While the EU is more open about how it approaches the classification, transfer and sharing of information, NATO tends to be more privacy-oriented (Jacopo Maria Bosica, 2023).

Chapter 2: Current situation of cooperation between NATO and the EU

Although the relations between the two organizations had started since the 1990s, it was only at the beginning of the new millennium that the official foundations of this connection were laid. Officially, cooperation between NATO and the EU was established in 2002, through the NATO-EU Declaration on European Security and Defense Policy. Currently, the cooperation includes 74 projects that promote security, crisis management and training. The international crisis caused by the COVID-19 pandemic highlighted the importance of cooperation between the EU and NATO and, at the same time, between the military and civilian sectors. To face the general situation in 2019 and to overcome the crisis, NATO and the EU have closely collaborated with the aim of increasing medical interoperability and their operational readiness. In this sense, several exchanges of information took place, promoting a coherent, complementary and transparent work environment (European Union External Action, 2021).

Over the years, cooperation between NATO and the EU has increased and integrated new areas, but an important moment that amplified this connection was the annexation of Crimea by Russia in 2014, when they considered it necessary to adopt joint declarations, one from 2016 and one from 2018, through which they aimed to increase defense cooperation. In view of Russia's even more violent actions against Ukraine launched in February 2022, actions that both the EU and NATO condemn, the organizations signed, in January 2023, a third Joint Declaration to strengthen and expand the already existing partnership (NATO, North Atlantic Treaty Organization, 2023). Over time, the connection improved progressively, by planning joint exercises, exchange of information, exchange of personnel.

In addition, the NATO-EU partnership is currently strengthened by at least four common dimensions regarding security enhancement: increasing European military capability, improving military mobility and interoperability, sharpening cooperation in the cyber and disinformation space and identifying synergies in procurement through the securitization of technology and supply chains. Cyber cooperation between NATO and the EU is based on the Technical Arrangement on Cyber Defense, jointly developing training, research, information exchange and exercises. For example, in 2019, the NATO Secretary General participated in CYBRID, a hybrid exercise organized by the EU in Estonia, and EU representatives participated in other annual NATO cyber exercises. In addition, the two organizations plan and coordinate other similar exercises through which they aim to improve their knowledge of each other's working methods and their ability to coordinate. Furthermore, the two organizations have cyber incident response teams that exchange policy updates and best practices (European Commission, 2021).

In the military domain, NATO and the EU follow similar directions. Neither organization has its own military forces, but relies on the personnel and equipment that member states can make available, in the case of a mission initiated by NATO or the EU. In the last more than 20 years, NATO and the EU have moved from coexistence to cooperation in several areas. The strategy of the two organizations has aligned over the years, despite the different goals and objectives they pursue. For example, in 2022, NATO launched the 2030 Strategic Concept, through which it develops its security plans and intentions regarding threats such as terrorism, threats arising from global competition, climate change, disruptive technologies, cyber (Brzozowski, 2021). In the same year, the EU launched the Strategic Compass, which includes some of the issues that NATO also refers to in its 2030 agenda, such as slowing globalization, competition for power, regional instabilities, threats from state and non-state actors. (EUDefence, 2020).

NATO considers the EU to be a unique, essential partner with which it shares strategic interests and with which it faces similar threats and challenges. As we mentioned before, the organizations cooperate in areas such as crisis management, development capabilities, providing support to common partners in the east and south, and addressing challenges arising from increased strategic competition.

The development of European defense capabilities is a key element of the joint efforts to transform the Euro-Atlantic space into a safer area and is also a form of burden-sharing. In developing these capabilities, NATO member states must ensure coherence and complementarity. At this moment, 22 NATO member states are also EU members, which means that the strategic partnership between the two organizations is strengthened by a similar thinking regarding the need to ensure the security of the European space. For these reasons, joint activities are carried out, by the EU, through the EU's Capability Development Plan (CDP), Headline Goal Process (HLGP) and Coordinated Annual Review on Defense (CARD), and the respective NATO processes – NATO Defense Planning Process (NDPP) and the Partnership for Peace Planning and Review Process (PARP).

The two organizations collaborate including in the context of the development of multinational capabilities, within the defense initiative of the EU and NATO's multinational High Visibility Projects. Following Russia's aggression against Ukraine, the EU and NATO increased munitions cooperation, particularly in the land and air domains, with an increased focus on supporting Ukraine and replenishing member states' stockpiles.

In all areas in which NATO and the EU cooperate, both of them aim to come up with innovative solutions and, above all, to avoid unnecessary duplication of efforts (NATO, North Atlantic Treaty Organization, 2023).

Despite all the problems, the main way both organizations can excel is cooperation. Especially in recent years, military mobility has started to be seen as a good example that improves the connection between NATO and the EU, being the first PESCO project extended to NATO non-EU countries. However, we should not lose sight of the fact that this project, even if it is several years since it was initiated, is still at the beginning of the road and has quite a few limitations (Droin, 2023).

Chapter 3: The role of military mobility in the development of cooperation

Military mobility is *the ability to deploy and move troops across European territory* and is essential to projecting a credible deterrence, but also a key area where NATO-EU cooperation is beginning to succeed. However, there are several factors that slow down mobility and negatively impact the preparation of European space defence, such as incompatibility of infrastructure, complex rules regarding the transport of weapons or military equipment. In 2019, NATO countries have identified concrete steps that would help increase military mobility, with the aim of being capable of deploying 30 land battalions, 30 air squadrons and 30 combatant ships in the span of 30 days (NATO, 2019). These steps are focused on four areas: developing and strengthening infrastructure, improving strategic airlift and sealift capabilities, strengthening the line of command and control and planning for better large-scale coordination, and simplifying legal and diplomatic procedures in the military and civilian sectors to facilitate the process for granting approvals.

Although there was a desire for developing this project, NATO subsequently identified a series of gaps regarding resources and institutional weaknesses in tackling military mobility. This domain is very important for strategic projection, which is why it leaves space for a constructive dialogue between NATO and the EU (Giovanna De Maio, 2021).

Given the extensive experience and regulations drawn up at the EU level, the organization could play a decisive role in the implementation of military mobility projects by simplifying the processes of obtaining clearance for the transport of goods, materials and military personnel. The EU has also been involved in improving infrastructure, a key project for improving military mobility. In this sense, it launched the projects related to the Trans-European Transport Network (TEN-T), developed studies that aimed at eliminating bottlenecks to mobility (by completing the missing sections of the transit corridors, developing infrastructure projects that use dual-use technology) (European Commission, 2021).

In recent years, the EU has strengthened its financial and legal mechanisms to be more competitive when it comes to security. In this sense, in 2017, the European Council established the Permanent Structured Cooperation mechanism, which includes 46 projects in several domains, one of them being that of military mobility. The leadership of both organizations agrees that it is time to identify new ways to fill security gaps and effectively allocate resources to ensure troop training. The area of interest in this paper, which highlights the increased cooperation between NATO and the EU, is that of improved military mobility and interoperability.

It goes without saying that the military posture of the EU military forces is essential to the achievement of organizational objectives. Yet, equally important is the rapid deployment of these forces and their interoperability in the trans-Atlantic space. For this reason, NATO-EU cooperation becomes even more relevant, in the development of projects related to military mobility (Giovanna De Maio, 2021).

The NATO-EU partnership in the field of military mobility is essential for ensuring regional and international security, in the current geopolitical context. Both organizations strive to ensure a coherent approach to the issue. A Structured Dialogue on Military Mobility, bringing together key stakeholders of both organizations is crucial in this respect. Thus, the staff can discuss and share priorities, such as military requirements, transport infrastructure, the transport of dangerous goods, customs, cross-border movement permissions and relevant exercises, as well as development and updates of the EU's Military Requirements for Military Mobility within and beyond the EU (NATO, North Atlantic Treaty Organization, 2023). After the first

NATO-EU Joint Declaration signed in 2016, the two organizations showed common interest to ensuring the rapid deployment of military personnel, by sharing information, through the Structured Dialogue on Military Mobility. This is the main way NATO and the EU communicate about legal, procedural and infrastructure obstacles, border crossings, deployment in the event of exercises (Jacopo Maria Bosica, 2023).

Since the signing of the first NATO-EU Joint Declaration, the organizations have initiated several proposals in the field of military mobility and assumed several commitments. In 2018 and 2019, NATO and the EU shared their respective military requirements for infrastructure. After NATO sent the updated infrastructure parameters to the EU in 2019, the EU Council approved an update to the transport infrastructure parameters and the geographical data of military requirements within and beyond the EU in July 2019. In order to avoid duplication of work, NATO accepted the same model regarding the standards for the transport of dangerous goods in the European space. In 2021, to enhance cooperation, NATO shared its Main Supply Routes maps with the EU. Given that NATO and EU forces and capabilities are shared, these maps will ensure greater synergy between the two organizations (Hans-Werner Wiermann, 2023).

The project on military mobility seems to be effective for both organizations through the lens of the measures taken over the years in terms of infrastructure development or the reduction of bureaucratic barriers, as well as through the lens of the development of cooperation between NATO and the EU. In the Action Plan developed by the EU in 2018, the organization tasked the European External Action Service (EEAS) with developing military infrastructure requirements in Europe. This was carried out in cooperation, albeit informally, with NATO. NATO and the EEAS have established their common priorities in the field of military mobility (for example, NATO's focus on the development of east-west corridors).

The development of the military mobility project is not easy, due to the reluctant attitude of some member states and/or the EU or NATO. On the other hand, however, one reason why cooperation in the field of military mobility between the two organizations is effective is because there is no rivalry between the two and they make military mobility a priority (Margriet Drent, Kimberley Kruijver, Dick Zandee, 2019).

Through legislative measures, the simplification of procedures and diplomatic clearances to enable rapid crossing of borders, on land, in the air, and at sea, NATO has been able to improve the readiness of its forces, as well as increase their ability to move within Europe, in peacetime, crisis or conflict (Margriet Drent, Kimberley Kruijver, Dick Zandee, 2019).

After analyzing some relevant documents in this domain, which capture the general picture of NATO-EU cooperation or aspects regarding the importance and the manner in which military mobility has influenced this cooperation, we believe that future relations regarding military mobility could be presented under one from the following forms:

1. Increasing the exchange of information in the field of military mobility is only a first step, which could support the development of cooperation on other levels as well, forming a stronger and more formidable NATO-EU partnership than now;
2. Military mobility will be an important project for both organizations, which will be successfully completed, through the allocation of funds, human resources, materials, information exchange and common rules, but will not lead further to a new stage in the development of cooperation in other domains.

Taking into account the official importance of the analyzed sources, we tend to believe that the first option is the one that will be successful.

In order for the NATO-EU partnership to increase in value, with our experience accumulated so far, we propose a set of measures:

- The foundation of joint headquarters which will allow the exchange of information between the two structures;
- The precise establishment of common objectives and the appointment of specialists in the field creating working groups in order to achieve these objectives;
- Respect, on both sides, of the terms and obligations assumed regarding the fulfillment of the military mobility project.

Conclusions

To enhance coordination, each organization should consider how it can add value to the other, in military or non-military domains. During the years of partnership, the security environment was characterized by safety, peace, economic stability and the aim was to avoid duplication of decisions by the other organization. These things would not have been possible if each organization had not understood the role of the other and had not adapted to the requirements. In order to improve their work, each organization decided to examine itself so as to ensure that it remains focused on the purpose for which it came into being. NATO, through the NATO 2030 process, aims to take an integrated approach to resilience, allocate more funds for technological development, increase its partnerships and pursue the security implications of climate change. On the other hand, the EU, through the Strategic Compass, intends to increase security at the European level by defining future threats, objectives and ambitions in defense. These projects will be vital for the two organizations, taken individually, but also for their cooperation, to develop a common future, in which they understand the challenges and opportunities that may arise.

Strong cooperation between NATO and the EU is essential in the field of military mobility. Dialogue in this regard is important for information sharing in key areas of military mobility such as transport, infrastructure, customs, cross-border movement permissions, communication.

NATO and the EU are still looking for a way to better cooperation. Even if military mobility seems to be a good way to strengthen the ties between the two organizations, the time has yet to be found to ensure cooperation without borders. But, for this, what is required is desire, initiative, leadership and involvement from all actors. Considering the need to ensure the security of the European space and the common interest of the organizations in this regard, military mobility seems to be a promising project, which ensures not only an efficient infrastructure, which allows the movement of military forces from one point to another, rapid deployment in case of crisis or simply – moving to participate in military exercises, but also a key element in the development and improvement of cooperation between these organizations.

BIBLIOGRAPHY:

1. Brzozowski, A. (2021, 11 10). *Europe has to become a security provider says EU's Borrell*. Retrieved from Euractiv: https://www.euractiv.com/section/defence-and-security/interview/europe-has-to-become-a-security-provider-says-eus-borrell/
2. Crisis Group. (2021, 07 08). *International Crisis Group*. Retrieved from Rising tensions in the Eastern Mediterranean: https://www.crisisgroup.org/europe-central-asia/eastern-mediterranean/rising-tensions-eastern-mediterranean
3. Defence, E. (2022). *EU-NATO Cooperation.* Brussels: Strategic Compass.
4. Droin, M. (2023, 01 17). *Center for Strategic and International Studies*. Retrieved from NATO and European Union burden sharing: https://www.csis.org/analysis/nato-and-european-union-burden-sharing
5. EUDefence. (2020, 11). *EU Agenda*. Retrieved from Towards a Strategic Compass: https://euagenda.eu/upload/publications/towards_a_strategic_compass_20_november.pdf.pdf
6. European Commission. (2021). *European climate infrastructure and environment executive agency*. Retrieved from CINEA: https://wayback.archive-it.org/12090/20221205163723/ https://cinea.ec.europa.eu/index_en
7. European Union External Action. (2021, 07 01). *The diplomatic service of the European Union*. Retrieved from NATO and EU, strength in complementarity: https://www.eeas.europa.eu/eeas/nato-and-eu-strength-complementarity_und_en
8. Giovanna De Maio. (2021). *Opportunities to deepen NATO-EU cooperation.* Washington: The Brookings Institution.
9. Hans-Werner Wiermann. (2023, 06 20). *Cooperation is essential to European and global security*. Retrieved from Concordiam - Journal of European Security and Defense Issues: https://perconcordiam.com/the-nato-eu-partnership-2/
10. Jacopo Maria Bosica. (2023). *EU military mobility: an obstacle race to turn long-standing pledges into a defence policy flagship.* Finabel - The European army interoperability centre.
11. Margriet Drent, Kimberley Kruijver, Dick Zandee. (2019). *Military Mobility and the EU-NATO Conundrum.* Hague: Netherlands Institute of International Relations.
12. NATO. (2019, 10 24). *North Atlantic Treaty Organization*. Retrieved from Press Conference: https://www.nato.int/cps/en/natohq/opinions_169936.htm
13. NATO. (2023, 11 30). *North Atlantic Treaty Organization*. Retrieved from Relations with the European Union: https://www.nato.int/cps/en/natohq/topics_49217.htm

1053477-3045-1396-24-30

PARTICULARS REGARDING TEACHING STYLE IN MILITARY PHYSICAL EDUCATION

Alin-Dumitru PELMUȘ, PhD.
Colonel Associate Professor PhD, ”Carol I” National Defence University,
Bucharest, Romania
E-mail: pelmusalin@yahoo.com

Ion ANDREI, PhD.
Colonel Professor PhD, ”Carol I” National Defence University,
Bucharest, Romania
E-mail: ionandreiunap@yahoo.com

Abstract**:** *The topic addressed in this paper, namely the teaching style in military physical education, has been rather little addressed and studied by specialists in the field. Therefore, in the first part of the article, the teaching style valid for any instructive-educational process is conceptualized and defined, according to the specialized literature. Then, based on the contributions of psycho-pedagogical researchers, the typology and classification of the teaching style in general, but also specific to the teaching process in the field of physical education, are presented. In the second part, the aspects related to the teaching style in the field of military physical education are addressed. Considering the fact that in order to fulfill the objectives set by this category of instruction, a particularly complex training process must be completed, the main purpose of the article is to determine the specialists in the field of military physical education not to focus on a certain educational style, but to try to adopt a combined one, adapted to the needs of the group, level and stage of training.*

Keywords**:** *teaching style, military physical education, instructor, teaching-learning process, training process*

Introduction

Teaching style is a concept imposed relatively recently in the psycho-pedagogical literature that mainly refers to the individual particularities of the teacher/instructor, to his own way of working, to the original way of training, choosing and using didactic strategies in his relationship with those he instructs. It practically represents the need to support a qualitative teaching performance through the instructor's ability to behave efficiently in order to fulfill the designed educational objectives.

The efficiency of the instructional-educational process is the result of the interaction of the set of factors and conditions that compete for its development. The personality of the instructor, of the educator himself, represents a filter that prints directions of action and nuanced purposes to the entire instructional approach.

1. Conceptualization and definition, typology and classification of teaching styles

The teaching style or didactic or educational style is a notion with much too broad meanings, since, until now, an insufficient process of conceptualization has been completed, to which is added a series of difficulties arising from the polysemanticism of the term. The definition of style is nuanced according to the different attitudes adopted by researchers in the pedagogical field, as several investigation paradigms are involved. Thus, depending on the generative sources and the origin of the styles, there are four conceptions to consider:

ideographic (the style comes from the personal vision of the teaching staff and is a construction or a product of it); *nomothetics* (the style comes from the specifics of the teaching activity and is the expression of didactic behavior based on internalized and personalized norms); *situational* (gives a causal role to the context); *ideothetic* (advances the hypothesis of the triple provenance of the style, as a synthesis or original combination of the three mentioned variables). This combination of factors explains the load of connotations that characterize the concept of teaching style (Cerghit, 2008, 314).

According to the *Pedagogical Lexicon*, the term style adopted by an educator in an instructional-educational process has three definitions, which essentially have the same meaning:

- didactic style – *”Behavior of the educator that denotes his way of applying the theory of instruction ... We often meet him in the works that study didactic style, in its various forms of manifestation.”* (Ştefan, 2006, 322);

- the educational style – *”Behaviour of the educator, which manifests itself not only in the strictly didactic framework, but in the educational process under all its aspects ... It is the expression of the originality of each educator (including parents here), of his special way of to be, but also of a pedagogical culture, of conceptions, opinions, mentalities. An old classification (starting from the leadership styles established by K. Lewin) refers to authoritarian style, democratic style and laissez faire style”.* (Ştefan, 2006, 323);

- the teaching style – *”Personal way, in which a teacher acts, constantly, in the instructive-educational process. The term teaching style has such varied meanings that it almost defies a clear definition (D.P. Ausubel). It is due to individual characteristics of the respective teacher, but it also depends on other factors (the social context, the norms of the school institution, the characteristics of the students they work with and of the teaching staff, etc.)”* (Ştefan, 2006, 323).

Regarding the typology of teaching styles, it should be noted that there is no pure style, but dominants or associations of dominants, which give configuration to hypothetical models or styles. The different classifications of the teaching style were based on several criteria that allowed the revelation of a wide and varied range of styles, gradually built around one or the same determinative variable. In this broad context of typology, the pedagogue Ioan Cerghit, synthesizing the data and contributions of researchers in the field, instead of insufficiently elaborated typologies, rather presents a list of such types of styles reflected in the didactic activity:

- *academic/heuristic* (focused on transmission, communication/focused on stimulating search, experimentation, discovery, research);
- *rational/intuitive* (based on scientific reasoning and systematic evaluation/focused on intuition, imagination, self-knowledge, spontaneity, pedagogical mastery);
- *innovator/routine prone* (open to new things, invention, creation, originality, ingenuity/ rigid, prone to repetition, reluctant to any innovation, dogmatic, having as a pretext one’s own experience);
- *informative/formative* (focused on the development of the students' personality, making the content a tool for practicing domain-specific thinking, making the most of the content's educational potential);
- *productive/reproductive* (based on divergent thinking, critical to the production of new/conformist, dogmatic, imitative);
- *deep/superficial*;
- *independent/dependent* (initiative, enterprising, overcomes difficulties, does not feel the need for help/hard analysis of the situation);
- *expository/Socratic* (with preference for dialogue);
- *descriptive/dialectical;*

- *analytical/synthetic;*
- *authoritarian/centered on autonomy* (centered on rigorous management/with independence granted to students, centered on their spontaneity);
- *imperative/indulgent* (demanding/low level of demand);
- *affective* or *empathic/distant* (close, warm, empathic/cold attitude, reserved);
- *self-controlled or self-censored/spontaneous* (calculated in everything, methodical/impulsive, disorganized);
- *solitary/of the team* (prefers to work alone/work in cooperation with colleagues);
- *focused on the teacher/focused on the student*;
- *elaborated/non-elaborated*;
- *motivating/non-motivating* (compensatory, rewards efforts, praises/does not stimulate curiosity, interest, passion, aspirations);
- *old/new* (with an inclination towards standardized forms/situated in the pedagogical current, proves flexibility, adaptability to changes);
- *predictable/unpredictable* (Cerghit, 2008, 318-319).

Regarding the field of physical education and sport, Mosston and Ashworth first conceptualized a spectrum of teaching styles, thus developing a coherent framework to serve as a guide for physical education teachers. This spectrum consists of eleven different teaching styles, five of which are teacher-centered (from the reproductive or direct style category) and six student-centered (from the productive or indirect style category). On the whole, these teaching styles allow for multiple approaches to teaching-learning act, such as behavioral and cognitive or related to peer teaching, peer assessment and self-assessment. Next, in the view of the above-mentioned authors, the eleven teaching styles are classified and described, as follows:

- *the command style* (Mosston, Ashworth, 2008, 76) – the teacher leads the instructional process and makes all the decisions, this style is often described as autocratic. The teacher provides the model and the students immediately respond to the stimulus. It is used when safety and time are of the essence or when quick responses are required and skills need to be replicated;
- *the practice style* (Mosston, Ashworth, 2008, 94) – the main characteristic of this style is the demonstration of the task by the teacher. This creates an opportunity for students to practice and develop skills at their own pace. In this sense, the teacher provides individual and group feedback while the students complete the tasks prescribed by him;
- *the reciprocal style* (Mosston, Ashworth, 2008, 116) – the defining characteristics of this style are social interactions, reciprocity, receiving and giving immediate feedback, guided by specific criteria provided by the teacher. Specific to the mutual style are exercises with a partner. Thus, students work together in pairs, complete the task and observe each other in turn. They also provide feedback to each other using performance criteria according to the skill sheet designed by the teacher. At the end of the first exercise, the performer and observer switch roles and the teacher provides feedback to and through the observer;
- *the self-check style* (Mosston, Ashworth, 2008, 141) – it is similar to the reciprocal teaching style, except that students work individually. The characteristic of the style is the execution of the task by engaging in self-assessment guided by the performance criteria/skill sheet provided by the teacher. This skill sheet includes a visual reference for correcting errors;
- *the inclusion style* (Mosston, Ashworth, 2008, 156) – the role of the teacher is to plan and set a varied range of tasks with differentiated levels of difficulty. The role of the learners is to analyze the level of availability in carrying out the task, to decide which is the most suitable task for their abilities and motivations;
- *the guided discovery style* (Mosston, Ashworth, 2008, 212) – according to this style, the teacher logically and sequentially designs a series of questions and tasks that lead students to discover a predetermined answer to a problem or learning target;

- *the convergent discovery style* (Mosston, Ashworth, 2008, 237) – similar to the guided discovery style, except that in this case the problem or question set by the teacher has only one correct solution. The students' role is to engage in reasoning, to control the learning process using trial and logic to discover the correct answer;
- *the divergent discovery style* (Mosston, Ashworth, 2008, 247) – represents the progression from the convergent discovery style. Basically, the teacher plans a single question/situation, the students being challenged to offer divergent answers with multiple possible solutions. This style can be effectively approached when teaching the tactics of sports games, gymnastics, athletics etc.;
- *the learner-designed individual program style* (Mosston, Ashworth, 2008, 274) – this style is characterized by the independence of each student to design his individual program by discovering the structure that solves the problem, the teacher being only the decider of the area of interest, which the learner must develop. In approaching such a style, it must be taken into account that it is necessary for students to have good knowledge and creativity in the field. Students should also have experienced other teaching styles, demonstrate independence in learning and, if necessary, be able to rely on teachers' expertise;
- *the learner-initiated style* (Mosston, Ashworth, 2008, 283) – similar to the design style of the learner, the learner's role is to independently initiate the behavior, decide on the initial area of focus, and design his own learning program in relation to his cognitive and practical ability. The teacher's role is to accept the learner's availability. The characteristics of the teacher who approaches this teaching style are: the ability to make maximum decisions in the learning process, the quality of being supportive and effectively participating in the instructional process according to the student's requests;
- *the self-teaching style* (Mosston, Ashworth, 2008, 290) – the defining characteristic of this style is independent/individual learning. Through tenacity and desire to learn, students must take full responsibility and make all decisions for their own development in the learning process.

Regarding the didactic of physical education in Romania, Professor Adrian Dragnea together with his collaborators, prominent specialists in the field in our country, consulting the specialized literature, categorize the teaching style as follows:

- *the direct teaching style* – this represents the traditional approach to teaching physical exercises, in which the teacher is the one who makes the decision of what to do and when to do it. This teaching style presents a number of advantages (practice efficiency and reducing the chances of subject error in performing a motor task; structuring the learning environment allows good control of the subject group, therefore it is recommended for working with large groups), but and disadvantages (the impossibility of differentiated treatment of subjects, depending on the biomotor potential of each one, of capitalizing on creativity and personal initiative; focusing especially on the learning results and not on the process that takes place). The training methods specific to this style are: *the command method* and *the task formulation method*. *The command method* consists of going through the following stages: explaining and demonstrating the motor action to be performed; the execution of the subjects, before they are given other instructions; correcting typical mistakes; providing methodical indications; correcting atypical mistakes; resuming the execution of the motor action. In this case, the teacher permanently controls the practice of the subjects: the beginning, the progress, the end of it. T*he task formulation method* is similar to the command method because the teacher specifies what and how to practice. Its use, however, allows subjects a greater degree of freedom in decision-making. In the use of this method, the following training sequences are encountered: the differentiated explanation and demonstration of the execution mode of the motor skill depending on the level at which the subjects are, divided into groups; differentiated execution according to possibilities; correcting individual mistakes and stimulating subjects to move to a higher level. This method encourages evaluation and self-evaluation, stimulating active and conscious participation, by setting individual training objectives.

- *indirect teaching style* – in this style, the teacher uses teaching methods centered on the student's activity. This teaching style is based on the idea that learning can be achieved through problem solving, experimentation and self-discovery, and the student has the freedom to choose the way to solve the motor task. The methods subordinate to this style are: *the exploratory method* and *the method of learning through discovery*. *The exploratory method involves*: asking the students to solve a certain motor task, without specifying the way to solve it; any solution presented by the students can be accepted; the teacher does not demonstrate, does not give verbal instructions, leaves it up to the students how to solve the motor task. *The method of learning through discovery* stimulates the students' creativity as follows: the teacher encourages the students' initiative, but the presentation of the work task changes; there is also the phase of observing the execution of the other subjects, so that the students are able to appreciate their own execution, in relation to that of their colleagues (Dragnea and collaborators, 2006, 163-165).

The combination of direct and indirect teaching styles is reflected by the limiting method, which combines the particular aspects of the methods presented above. Thus, the teacher can use the indirect style, in the sense that he asks the subjects questions or puts them in a situation to solve problems, but at the same time leads them in solving the tasks through precise instructions, specific to the direct style. This combined teaching style is very effective in teaching motor skills, regardless of the stage of their formation. The limiting method, as a sequence of training sequences, is presented as follows: free exploration; discovery learning; problem solving; precise instruction forms (Dragnea and collaborators, 2006,165).

2. Aspects of teaching style in military physical education

Similar to school physical education, the teaching activity *"...in military physical education is defined as the activity of transmitting a content to be learned, theoretical and/or practical, specific to the educational or training activity. Concretely, it involves the presentation of the content, the explanation of the essential aspects of the notions, the development of practical and theoretical skills, all based on the objectives and purposes of this activity and of the social order. The efficiency of teaching is also conditioned by the style approached by the specialist in military physical education"* (Ciapa, 2019, 72). However, unlike school physical education, *"military physical education is the starting point of the entire process of training for combat, the pivot of the other components of the training, which determines the efficiency of the military in carrying out combat missions and the efficiency of peacetime activities"* (Romania Defence Staff, 2021, 8).

In the field of physical education and sports in the army, there are several ways of manifesting the instructor in the particularly complex teaching-learning process. These modes of manifestation are carried out depending on the characteristics of the instructor's personality, but also in relation to the characteristics of the recruits /military pupils/cadets/students, given their particularities of age, gender and aptitude. So, as it happens in all training processes, also in military physical education the teaching-learning actions differ from one instructor to another, even if the thematic contents in the activity planning documents are mostly identical. These differences are due to the decisions that each instructor adopts when designing the training session, decisions that define his teaching behavior, therefore outline his teaching style.

It is obvious that instructors face the most important challenge in the field of didactics: to scientifically know how the military develops and accumulates knowledge, in order to achieve an effective training process. Taking into account the diversity of didactic methods and strategies used during professional training for the purpose of training specific skills, future military instructors/teachers must accordingly personalize their behaviors and teaching styles in order to achieve the instructional-educational objectives. At the same time, the didactic techniques must be adapted according to the specifics of the physical education activity in the respective military structure, the training objectives of the sessions, the available material base and the particularities of the group. Based on these styles, it is possible to determine the level of participation and the degree of involvement of any training soldiers (recruits, pupils, cadets, students) in the act of learning, the independence and autonomy shown in decision-making during the training session, the relationships that develops within the collective. Also, these styles have effects on the instructor as well, he being forced to select a teaching style centered on the military pupil/cadet/student in accordance with the requirements of modern didactics, which stipulates that this is considered the main pole of training.

In order to maintain an optimal state of health of the personnel and, implicitly, to increase the operational capacity of the forces, there is a need to instill in the military the appropriate techniques for applying a wide and varied set of motor skills, i.e. developing their ability to practice physical exercise independently during individual physical training and in free time (autonomy or motor self-training capacity). Also, techniques to motivate the military in order to increase the level of physical training and their awareness about the benefits of physical education and sports on maintaining the operational capacity of the structures become imperatively necessary. However, however motivated and aware the military may be of the benefits of physical education, motor autonomy or self-training must be preceded by a thorough training by the instructor, which turns with time into discrete coordination. This specific style of military training is also applied to the level of physical education activity in high school and university education, but especially to the level of performance sports.

In military education it is very easy to limit yourself. Once you reach a certain didactic level in education or instructor with a higher military rank you have a natural tendency to stop. Either this means adopting one of the ineffective teaching styles (routine, distant, unmotivating, undeveloped), with the teaching of repetitive training sessions, from memories, which do not keep up with developments in the field and, above all, with the realities of troops training. In order not to get here, it is absolutely necessary, in addition to the continuation of the scientific research effort, to collaborate with fellow specialists in the field through certain learning networks, to participate, in whatever form, in various activities related to the specialty (conferences, seminars, workshops -s, convocations, working groups, etc.), sports events organized at local, national or international level and, especially, at sports and military-applicative competitions. Participating in such activities enables military physical education majors to share ideas with others and at the same time receive feedback on their ideas. In this context, a specialist in the field belonging to the specialized university environment in our country states that *"The best teachers of physical education and sports, within the universities, maintain a growth mentality, always looking for ways to improve through their own professional development"* (Tudor, 2001, 122).

In order not to limit oneself, it is very important for any military physical education specialist to diversify both the means with which he acts in the physical education sessions, and the sports tests in the competitions organized at the level of each structure in which he carries out his activity. A quality military teacher/instructor must be available. It is very easy to say that these are the means with which they operate at the level of the department/teaching committee and to indulge in this situation, without trying to diversify the training program. Also, despite the fact that the material basis of instruction in the field of military physical education does not, in many cases, meet the quantitative and qualitative standards, the teaching staff must adapt the means of action that they have at their disposal for conducting training sessions as attractive as possible.

Within a study program, a teaching style must be approached that determines, after its completion, a desire of the graduates to remain close to the instructor who trained them, regardless of what level of training. The feedback, the close connection between the graduate of the study program and the teacher represents his greatest satisfaction. The level of satisfaction, the well-being of the teacher tends to reach the absolute when graduates express their gratitude and appreciation for his efforts, hearing from them that what they have learned has become useful to them, their interest in a particular issue has been stimulated (practicing physical exercise in our case) and remembering with great fondness the time spent together. When these links are created between the graduates and their teachers, regardless of the communication channels, the didactic activity can be really improved, thanks to the discussions about what works in optimal conditions, what should be changed etc.

In order to approach an adapted teaching style in military educational institutions in which a process of training and continuous professional development is carried out, it must be taken into account that it is possible that the military being trained has, in some situations, a motor capacity better than that of the instructor, to have a lot of other interpretations and experiences acquired within the activity carried out at the structure where he comes from or, above all, within the international missions in which he participated. In cases of this type, pedagogical tact, pedagogical mastery must intervene, i.e. a teaching style adapted to the moment, through which the instructor can make the well-prepared military man to understand that the one targeted by the current program is military personnel who do not demonstrate an optimal level of physical training. In this context, it must not be forgotten that modern education is centered on the student as an axis around which everything gravitates, and the instructor must adapt his means of action to the needs of the one he instructs and take into account his interests and inclinations. From this point of view, the ability to communicate with a group of military personnel represents another fundamental component of the pedagogical skill. The communication act concerns the instructor's ability to transmit, through verbal and non-verbal means, the system of knowledge and motor skills, so that the act of communication is an active, dynamic and expressive one. Adopting a boring and uninteresting communication act produces a negative feedback from both well-trained and less-trained soldiers. The quality of teaching knowledge in the field of military physical education depends on the content and verbal fluency, but also on the personal example in the execution of motor actions, equally. At the same time, the trainer should not be afraid to ask questions and challenge assumptions, if they prove to be beneficial to the trainees.

The choice of teaching style is an aspect of the instructor's autonomy, but in military physical education it depends, to a large extent, on the target group of the training process. Therefore, in the following, some aspects are presented regarding the choice of certain styles in the extensive teaching-learning process of military physical education:

- instruction of subunits (platoon, company/similar), basic military training or other military training modules for cadets/students, courses that require high psychophysical effort, are stages of training in which not only in military physical education, but also in the other categories of instruction, an authoritarian teaching style should be approached with a preponderance;
- within the initial training programs of military personnel and those of continuous training carried out at the tactical level, it is indicated to use a combined teaching style from most of the styles appreciated by the instructor as effective. Also, the teaching style must be adapted to the time and period of instruction;
- in the physical education process carried out in headquarters and within the professional continuous development programs carried out at the operational and strategic levels, the effective option is the choice of a combination of educational styles such as

academic, rational, centered on autonomy, innovative, affective, but, at the same time, while maintaining an increased level of exigence.

The specialist in military physical education, regardless of the military structure in which he works, is put in the position to prepare from a psycho-physical point of view the military personnel at the beginning of the military career until to the retirement. Actually, it is obvious that for acquiring the components of physical training necessary to train the fighter (athletics – running/jumping/throwing technique; gymnastics – basic, acrobatic; swimming – free, equipped with the equipment provided, with improvised means of passing of the rivers; mountaineering – natural and artificial climbing/traversing/descending; combat sports – basic striking/blocking/throwing/strangulation/dislocation/immobilization techniques, hand-to-hand fighting techniques with/without equipped weapons; skiing – elements from the technique of cross-country/alpine skiing with the weaponry and military equipment, etc.) a certain combination of teaching styles is necessary, and for to maintain the qualities and motor skills (fitness elements, sports games) in order to increase the operational capacity of the forces, any other combination.

Conclusions

It should be highlighted that in military physical education, being an extensive and complex training process, a preferred teaching style should not be used, but rather a scheme of the integrated contribution of styles, which offers the instructor a varied range of didactic tactics and behaviors. The efficiency of the training process is closely related to the ability and mastery of the instructor to use the style according to his personality to achieve his designed goals.

The instructor/specialist in military physical education is the indispensable factor, he is the one who must operate with all aspects of modern didactics and establish differentiated objectives. Also, he must develop the most effective didactic strategies that lead to the achievement of each set objective. The efficiency and success of the instructional-educational process are ensured by a knowledge of all teaching styles, but also by an application in a combined and appropriate way for the group or the training stage.

BIBLIOGRAPHY:

1. Cerghit, Ioan. 2008. Sisteme alternative și complementare: structuri, stiluri și strategii, Ediția a II-a revizuită și adăugită. Iași: Editura Polirom.
2. Ciapa, Gabriel. 2019. Planificare și stiluri de predare în educație fizică militară. București: Buletinul Universității Naționale de Apărare nr. 3.
3. Dragnea, Adrian și colaboratori. 2006. Educație fizică și sport – teorie și didactică. București: Editura FEST.
4. Mosston, Muska and Ashworth, Sara. 2008. Teaching Pysical Education. First Online Edition, SUA: Spectrum Institute for Teaching and Learning.
5. Statul Major al Apărării. S.M.Ap.-40/29.06.2021. Concepția de educație fizică și sport în Armata României. București.
6. Ștefan, Mircea. 2006. Lexicon pedagogic. București: Editura Aramis Print.
7. Tudor, Virgil. 2001. Evaluarea în educația fizică școlară. București: Editura Printech.

1053477-3045-1396-24-31

ANALYSIS OF THE CURRENT SECURITY ENVIRONMENT THROUGH VUCA

Valentin-Lucian MAFTEI
Lieutenant (N), Master's Degree Student, Command and Staff Faculty, Navy Department, National Defense University "Carol I", Bucharest, Romania
E-mail: vmaftei88@gmail.com

Raluca Elena RADU
Lieutenant-commander, Master's Degree Student, Command and Staff Faculty, Navy Department, National Defense University "Carol I", Bucharest, Romania
E-mail: eralucaradu@gmail.com

Abstract: *The current security model and its trends bring to the fore ever more diverse challenges on global security. Thus, we are talking about an unpredictable and rapidly fluctuating environment, in which the decision-makers are facing sudden and complex changes, and the classical approaches becoming increasingly inadequate. In this article, we intend to analyze the specific challenges of this new security context, characterized by VUCA (volatility, uncertainty, complexity, ambiguity), and to identify possible forms of response to these challenges.*

Following the first direction, we will highlight the influence of VUCA on the current security environment by analyzing the 4 dimensions: volatility, uncertainty, complexity, and ambiguity. Volatility in security is fueled by geopolitical changes, regional conflicts, climate change, and the rise of non-state actors such as terrorist groups and evil cyber organizations. Uncertainty adds another dimension by the difficulty of anticipating changes and making precise threat assessments. The complexity of security comes from the interconnections between actors and risk factors, including, requiring multidisciplinary approaches and international collaboration. Ambiguity in threat assessment can lead to suboptimal decisions and can be amplified by disinformation and propaganda.

In the second direction, we will highlight the need for adaptive strategies to be flexible, and resilient, and to include international collaboration in order to successfully respond to VUCA challenges. The use of advanced technology and the development of anticipation and risk management capabilities are also essential in this context.

At the end of the paper, we will argue that adaptive strategies are crucial in the VUCA environment of global security, ensuring an effective and adaptable approach to dealing with threats in an uncertain and ever-changing world.

Keywords: *VUCA, mediul de securitate, strategii adaptive.*

Introduction

In the contemporary era, accelerated technological advances such as artificial intelligence and robotics are producing extreme changes in society, on organizations, regardless of their size. This new reality, increasingly defined as „an illusion created by the inability to forecast" (Cioranu 2021, 1), requires the need to identify new methods of managing potentially chaotic situations.

Global and national security is therefore in constant transformation and adaptation. The current security environment is defined to a large extent by the term VUCA, an acronym that denotes Volatility, Uncertainty, Complexity, and Ambiguity, reflecting the profound and rapid changes that influence both national states, as well as global communities. This concept, originally used in the military context, has become increasingly relevant in the fields of politics, economics, and security, posing a major challenge for policymakers and analysts around the world. (Tuleja E.A. 2017, 195)

The term VUCA was originally used in the military context to describe the changing and unpredictable nature of modern operational environments where the armed forces must adapt quickly to complex and dynamic challenges. This concept was later adopted in the field of business and management to highlight the need to develop flexible and resilient strategies in the face of uncertainties and rapid changes in the global business environment. In the military environment, the application of VUCA principles has led to the development of more agile approaches and the improvement of strategic planning and decision-making capabilities in uncertain conditions.

Volatility in the security environment is manifested by sudden and unpredictable changes, generating unexpected risks and opportunities. Events such as geopolitical conflicts, financial crises, or the emergence of new non-state actors can disrupt the status quo of global security.

Uncertainty is becoming a central factor in security decision-making, as government actors and organizations must adapt to ever-changing scenarios. Uncertainty can be fueled by political, economic, or technological developments, which can substantially influence security strategies and objectives.

The complexity of the current security environment derives from the complex interlinkages between threats, actors, and interests. Factors such as transnational terrorism, forced migration, or cyber threats add a degree of difficulty in assessing and managing risks.

Ambiguity accentuates the difficulty in addressing security. Contradictory information and misinformation can create confusion in the decision-making process, and multiple interpretations of the same data can generate uncertainty and suboptimal decisions.

Faced with this VUCA environment, traditional security approaches are becoming increasingly inadequate, and rigid strategies can become counterproductive. The article aims to explore the ways in which national states, international organizations, and civil society can develop adaptive strategies to meet the challenges of global security and ensure stability and prosperity in a rapidly changing world.

1. Volatility in security

Volatility is one of the defining aspects of the contemporary security environment and significantly influences how national states, international organizations, and non-state actors address threats and risks. The term VUCA, which denotes Volatility, Uncertainty, Complexity, and Ambiguity, perfectly describes the current security environment.

Rapid and unpredictable changes in the security environment are evident in a number of contexts. A well-known example is the evolution of geopolitical conflicts, where tensions can escalate sharply and lead to regime changes or the onset of wars. Volatility in global security is fueled by a number of factors, such as growing geopolitical rivalries, regional conflicts, climate change, and pandemics, all of which contribute to significant uncertainties and risks.

Volatility can also manifest in the economy, affecting the stability and prosperity of nations. Financial crises may erupt unexpectedly, affecting markets and creating uncertainty about economic sustainability. This economic volatility can have serious consequences for social and political security.

In addition, the rise of non-state actors, such as terrorist groups and malicious cyber organizations, adds another layer to global volatility. These actors can cause massive disruption through cyber attacks, propaganda, and international terrorism. These actors can act quickly and flexibly, changing their tactics and objectives according to developments in the security environment, which adds a significant element of volatility. (SRI 2021)

To deal with this volatility, security policymakers need to adopt flexible and adaptable approaches. A constant re-evaluation of security threats and strategies, as well as the development of anticipation and rapid response capacities, is essential. International cooperation is also becoming crucial in addressing global threats, as no nation can cope with such complex and unpredictable volatility on its own.

In conclusion, volatility in security is a contemporary reality, and policymakers must be prepared to adapt to the rapid and unexpected changes that can affect the stability and security of nations and the world as a whole.

2. Uncertainty and security

Uncertainty is a fundamental element in the current security environment, bringing with it significant challenges for national states and the international community in managing threats and risks. In the context of VUCA (Volatility, Uncertainty, Complexity, and Ambiguity), uncertainty is a persistent feature of global security.

Security expert Richard Haass notes: "Uncertainty defines many aspects of global security today. It is difficult to predict exactly what will happen in a world with so many variables" (Richard Haass 2008, 44). This is evident in a number of security aspects, including unexpected political developments, unpredictable economic and social events, and rapid changes in technology.

Uncertainty can be fueled by political instability at the international level or by changes in governance, which can have an unpredictable impact on international relations and on the behavior of states. Moreover, non-state actors such as terrorist groups or cyber hackers can take advantage of uncertainty to advance their own interests and goals.

In the economic field, uncertainty can affect the financial stability and prosperity of nations. Economic events, such as financial crises or fluctuations in global markets, can create uncertainties related to the economic viability of nations and influence domestic and foreign policy.

To deal with this uncertainty, states, and international organizations need to develop flexible and adaptable strategies. There is a need to strengthen capacities to anticipate change and manage risk in an unpredictable world. In addition, international collaboration is becoming even more important in promoting security and stability, as no nation can solve all challenges in such an uncertain environment alone.

To conclude, uncertainty is a defining feature of the contemporary security environment and requires flexible and adaptable approaches from decision-makers. Developing security strategies and policies that take this uncertainty into account is crucial to maintaining global stability and security.

3. Complexity in security

Complexity is a defining feature of the current security environment, bringing with it multiple interconnected aspects that influence how national states and international organizations respond to threats and risks. In the context of VUCA (Volatility, Uncertainty, Complexity, and Ambiguity), the complexity of security manifests itself in a variety of ways.

One of the key aspects of complexity is the interconnection between different actors and risk factors. For example, regional conflicts can have global repercussions, and climate change can affect global economic and social stability. International security can no longer be understood in isolation. It is a complex equation in which internal and external factors intersect in an unpredictable manner (Gabriel Rus Schupler 2021).

Another aspect of security complexity is related to rapid technological developments and globalization. Emerging technologies such as artificial intelligence or cyber technologies can create new threats and change the dynamics of international conflicts. Globalization also means that events taking place in one part of the world can have a direct impact on other regions, which brings an additional degree of complexity.

In order to cope with this complexity, policymakers need to develop integrated and multidisciplinary approaches in the field of security. This involves collaboration between various areas, such as national security, economic development, and crisis management. Security expert Thomas Wright points out: "Solving security problems in the 21st century requires complex and coordinated approaches that respond to today's challenges". (Thomas Wright 2018)

In addition, policymakers need to be able to anticipate and respond to emerging challenges and be open to adaptation. Developing risk assessment and crisis management capacities is becoming essential in such a complex environment.

To summarize, the complexity of security is a defining feature of the current global environment, and traditional approaches are no longer sufficient to meet this challenge. Developing integrated, multidisciplinary, and adaptable strategies is crucial to managing threats and risks in a world of rapid interconnection and change.

4. Ambiguity in threat assessment

Ambiguity is a significant feature of the contemporary security environment, bringing complex challenges in terms of assessing and correctly understanding threats. In the context of VUCA (Volatility, Uncertainty, Complexity, and Ambiguity), ambiguity is a persistent feature that affects how policymakers approach security.

Ambiguity can be highlighted in the difficulty of obtaining clear and accurate information about threats or intentions of enemies. In this regard, the former director of the US National Security Agency, Keith Alexander, notes: "In the digital age, information can be manipulated and disseminated quickly, he said, and ambiguity becomes a major problem in the assessment of "cyber threats". (Keith Alexander 2012)

Ambiguity can also be manifested in multiple interpretations of the same data or events. This can create confusion and make it difficult to make informed security decisions. In security, ambiguity can create major vulnerabilities, as misinterpretations of situations can lead to suboptimal decisions or underestimation of threats. (Colin S. Gray 2002)

Ambiguity is also fueled by disinformation and propaganda, which can distort perceptions and create a distorted view of reality. State or non-state actors can use these techniques to confuse and disorient opponents and advance their own goals. Information ambiguity and disinformation are increasingly used tools in the arsenal of cyber and hybrid threats. (John T. Watts 2023)

To address ambiguity in threat assessment, policymakers need to develop robust intelligence analysis and source verification capabilities. Collaboration and exchange of information between nations and organizations are becoming crucial to obtain a clearer and more complete picture of the situation.

In conclusion, ambiguity is a significant challenge in assessing threats in the current security environment. Policymakers need to be aware of this persistent trait and develop intelligence analysis and verification capabilities to make informed decisions and manage threats and risks more effectively.

5. Adaptive strategies in the VUCA environment

In the face of the VUCA environment (Volatility, Uncertainty, Complexity and Ambiguity), developing adaptive strategies is becoming essential to meet the challenges of global security. This fast-changing and unpredictable environment requires flexible and resilient approaches to ensure stability and security.

One of the key aspects of adaptive strategies is flexibility. Security experts stress the importance of being able to quickly adjust tactics and strategies in the face of unexpected changes. Solving security problems in the 21st century requires complex and coordinated approaches that respond to today's challenges. (Thomas Wright 2018)

Flexibility also involves the ability to learn from experiences and make adjustments based on these lessons. Organizations and governments need to be open to critical assessments and continuously improve strategies and capabilities to deal with the evolving VUCA environment. Resilience is another key element of adaptive strategies. It involves the ability to resist and recover quickly after crisis events or situations. Organizations and states need to develop crisis management capabilities and have sound response plans in case of unexpected events.

International collaboration is becoming crucial in the VUCA environment. No nation or organization can face global challenges alone. Cooperation at the international level can contribute to the exchange of information, resources, and experiences, thus enabling the development of more effective solutions to common problems. With the evolution of technology and the global communication environment, cooperation is becoming more accessible and necessary than ever.

The use of advanced technology can also play a significant role in the development of adaptive strategies. Emerging technologies, such as artificial intelligence and data analysis, can help to anticipate and manage risks and threats more effectively. Technology can provide significant opportunities in anticipating and preventing threats.

In the current security context, marked by unpredictability and rapid change, adaptive strategies are becoming crucial. They enable organizations and states to respond effectively to emerging threats by continuously adjusting and reconfiguring action plans. Their importance lies in the ability to anticipate changes, learn from experiences, and develop resilience in the face of adversity. The implementation of adaptive strategies also facilitates international collaboration and the integration of advanced technologies, essential to successfully navigate the complexities of the contemporary security environment.

To sum up, adaptive strategies are becoming increasingly important in the VUCA environment of global security. Flexibility, resilience, international collaboration, and the use of advanced technology are key elements of these strategies. In order to ensure stability and security in the face of ever-changing challenges, policymakers need to adopt proactive and adaptable approaches that enable rapid adaptation to security developments. The development of strategically-minded officers will have to focus on expanding education beyond professional training, on the development of attributes that allow them to imagine and implement these adaptive strategies.

Conclusion

In light of the VUCA environment (Volatility, Uncertainty, Complexity, and Ambiguity) that characterizes contemporary global security, adaptive strategies become essential to ensure national and international stability and security. This new security paradigm calls for flexible and multidisciplinary approaches that enable decision-makers to face the unpredictable and complex challenges they face.

The volatility of security is evident in the rapid and unpredictable changes that can affect the global security situation. Geopolitical conflicts, technological development, and the rapid development of non-state actors have a crucial role to play in increasing volatility. This volatility requires rapid anticipation and adaptation capabilities to respond effectively to emerging challenges.

Uncertainty, characterized by the difficulty of anticipating changes and making accurate assessments, adds an element of complexity to the decision-making process. Developing risk assessment and uncertainty management capabilities is essential for developing adaptive strategies.

The complexity of the security environment is due to the interconnections between different actors and risk factors. Traditional approaches are no longer appropriate in the face of this complexity, and international cooperation and integrated strategies are becoming crucial to meet the challenges.

Ambiguity in threat assessment can generate suboptimal decisions and amplify confusion. The development of intelligence analysis and source verification capabilities is crucial to achieving a fair threat perspective.

Adaptive strategies, involving flexibility, resilience, international collaboration, and the use of advanced technology, are the answer to the VUCA environment. In an ever-changing world, policymakers need to be prepared to adapt and develop proactive approaches to ensure security and stability. By developing adaptive strategies, we can address global security challenges more effectively and ensure that our society remains safe and protected.

BIBLIOGRAPHY:

1. Cioranu, I., Gândirea critică în leadershipul militar, revista *Colocviu Strategic*, nr. 14, 2021, p. 1.
2. Colin S. Gray, "Thinking Asymmetrically in Times of Terror," Parameters 32, no. 1, 2002
3. Gabriel Rus Schupler, Securitatea, între concept și drept cetățenesc, 2021.
4. Richard Haass, The Age of Nonpolarity: What Will Follow U.S. Dominance?, Foreign Affairs, Vol. 87, No. 3 (May - Jun., 2008), pp. 44-56 (13 pages).
5. Thomas Wright - The Return of Great Power Rivalry was inevitable, 2018.
6. Tuleja, E.A. (2017), "Cultural Intelligence in a VUCA World", Elkington, R., Steege, M.V.D., Glick-Smith, J. and Breen, J.M. (Ed.) Visionary Leadership in a Turbulent World, Emerald Publishing Limited, Leeds, pp. 195-227.
7. Keith Alexander, https://www.c-span.org/video/?306956-1/cybersecurity-threats-us, accesed 1st of February, 2024.
8. John T. Watts, https://www.atlanticcouncil.org/in-depth-research-reports/report/evolving-cooperative-security-approaches-for-tomorrows-realities/, accesed 1st of February, 2024.
9. SRI, https://www.sri.ro/cyberint, accesed 1st of February, 2024.

1053477-3045-1396-24-32

UNCONVENTIONAL ACTIONS MAJOR IMPACT FOR FREEDOM OF NAVIGATION IN CONFLICT AREAS

Valentin – Marian TOMA, PhD.
captain (Navy), Command and Staff Faculty/Strategic Command
Commanding Officer of „Mărășești” – 111 Frigate, Constanța, Romania
E-mail: valentintomita@yahoo.com

Abstract: *Navies were primarily created for the protection of merchant trade, with the mission of ensuring freedom of navigation on communication sea lines so that nations could prosper from commercial trade. The unconventional actions of some state or non-state actors affect the freedom of navigation in certain maritime spaces and thus cause the emergence of regional security crises and implicitly the shaping of economic crises. In this article, we have selected three maritime spaces where state and non-state actors use unconventional actions to disrupt and even prohibit freedom of navigation for commercial vessels. The international community is aware of the danger posed by these unconventional actions and is responding promptly and decisively through the actions of their military vessels in order to provide an adequate response and maintain freedom of navigation.*

Keywords: *freedom of navigation, merchant trade, lines of communication, piracy, missile attacks, drift mines, drones, effects, unconventional actions.*

Preliminary Considerations

The maritime domain has been used since ancient times as a transport route by those who ventured at sea and has contributed significantly to trade, cultural, and technological exchanges between civilizations. Thus, over time, complex maritime transport networks were developed on the seas and oceans, simultaneously with the continuous development of the fleets of commercial ships.

The communities established along the coasts prospered due to trade and had to fortify their cities against invaders and develop military fleets to continue to trade safely on the sea lines of communication. Over time, the great European maritime powers began to explore vast expanses of water, and created new empires proving that "the sea is like a strategic road, an environment used by one nation to conquer and dominate another nation" (Geoffrey Till, 2013, p.33). With the help of fleets, maritime nations were able to develop and increase their overseas territories. (Adrian Filip, 2013, p.113).

Alfred Thayer Mahan believes that the main element of sea power is commercial trade, and warships have the role of ensuring freedom of navigation in order to develop trade.

According to expert estimates regarding sea trade, more than 80% of the volume of trade is carried out at sea. The use of the sea as a source of food developed the fishing industry and implicitly the appearance of specific industrial branches with an impact on the economic development of the states that own fishing fleets.

In different maritime areas around the globe, especially in maritime areas with intense commercial traffic, since peacetime, a series of threats can appear that can limit the freedom of navigation, forcing commercial ships to adopt a series of safety measures or change travel routes.

The maritime domain is characterized by complexity and ambiguity, especially in maritime areas where asymmetric threats have significantly increased affecting freedom of navigation with economic implications both regionally and globally.

The main proposed objective of this article is to analyze the impact produced by the actions of state and non-state actors regarding the freedom of navigation in the maritime areas in which they act. In support of this approach, I chose the case study as an empirical research method.

Unconventional actions are undertaken by state or non-state actors who, in order to achieve their political, ideological, or religious objectives, use asymmetric warfare methods and procedures. The main reason for such a practice is the lack of human, material, financial and informational resources in relation to those of government forces or those against whom they fight. (Teodor Frunzeti, 2013, p.8).

We have selected three maritime spaces where different unconventional actions that limit freedom of navigation frequently take place: in the Gulf of Aden and off the coast of Somalia through actions of piracy against commercial ships, strikes by Houthi rebels in the Red Sea, and the danger created by mines in the Black Sea as a result of the Russian-Ukrainian war.

Freedom of navigation is one of the oldest and most recognized principles in the legal regime governing maritime space. The United Nations Convention on the Law of the Sea (UNCLOS), adopted in 1982 in Montego Bay, established the fundamental legal principles for the governance of the seas and oceans and defines the right to navigation as the right of all states regardless of whether are bordering maritime or inland areas. According to the 1958 convention, the United Nations Convention on the Law of the Sea (UNCLOS), in article 87 it is stated that: "*The open seas are for all states, whether coastal or inland. The freedom of the open seas is exercised under the conditions specified by the provisions of the convention and the other rules of international law. It includes especially for states whether they are coastal or inland: freedom of navigation, freedom of fly-by, freedom to lay submarine cables and pipelines, freedom to build artificial islands, freedom of fishing, freedom of scientific research*" (UNCLOS, United Nations, p.53).

Economic progress has generated an unprecedented increase in the maritime transport of raw materials needed for industry, grain transport, and the exchange of finished products, becoming a particularly complex economic activity with a national and international character. Shipping has become vital to the global economy, with more than 50,000 merchant ships on the open seas moving, transporting various goods from one part of the world to another. (Seaman, 2018).

The safe passage of trade routes is disrupted in certain areas of the globe by unconventional actions of some actors with the aim of obtaining sums of money from the ransom of commercial ships through piracy actions, to prohibit the transit of some commercial ships by attacking them with missiles or to discourage commercial activities at sea through the use of drift mines.

The methods used by state and non-state actors to achieve their goals in maritime spaces in conflict zones are diversified and adapted to the possibilities of expression. Their actions are usually of low intensity, but due to the frequency with which they are executed and the methods used, they become a phenomenon with global implications that is difficult to prevent and manage.

I. Piracy in the Horn of Africa – international implications

The phenomenon of piracy has increased off the coast of Somalia and in the Gulf of Aden in the context of the instability of the forms of government and the fragmentation of the Somali state. Disputes between tribes or clans and religious frictions are the source of all internal problems. Between 1977 and 1991, three major conflicts took place in Somalia. The first conflict between 1977-1978 was with Ethiopia to control the Odagen region inhabited by Somalis. Somalia lost the war, and this fact led to the appearance of differences between the clans and began the struggle for power in several regions. The second major armed conflict began in 1981 between the Somali Army and members of the Somali National Movement for control of the northwestern region of Somalia. Following this conflict, the region was placed under military administration. This conflict later turned into a civil war, a war in which approximately 60,000 Somalis died, mostly members of the Issaq clan (the largest clan in the Horn of Africa), the main support of the Somali National Movement, and 400,000 Somalis took refuge in Ethiopia. (The Journal of Economic Perspectives, Vol.33, 2019). Ethiopia intervened in support of the Somali National Movement and other opponents of the ruling regime, triggering a new armed conflict starting in 1989 between the ruling forces and all opponents of the regime. The ruling regime of President Siyad Barre was overthrown in 1991, and since then Somalia has experienced political instability amid infighting between local leaders, with historic regions sinking into poverty, uncertainty, and disorder.

The inability of local self-governing authorities, poverty, lack of own legislation, and non-compliance with international legislation are the main sources of generating and maintaining piracy actions. Attacks on merchant ships occur predominantly in the Gulf of Aden throughout the year and off the coast of Somalia depending on monsoon seasons and logistical capabilities. The mode of action of the pirates in the Gulf of Aden is given by the use of fast boats (skiffs) using mainly infantry weapons caliber 7.62 mm machine guns, anti-tank grenade launchers type AG-7, and other types of light weapons. (Small Arms Survey, Somali Piracy, 2012, p.197). Light alloy metal ladders, boat hooks, and various types of ropes are used for boarding ships. Long-range attacks use GPS receivers for navigation, allowing attacks to be carried out over 1,500 miles from shore. In these cases, larger boats (motherships) are used, which are generally used for fishing, with large amounts of fuel and fast attack boats on board. After the capture of merchant ships, large sums of money are demanded to ransom the ships and crews. Piracy in the Gulf of Aden and off the coast of Somalia must be viewed in the context of the close ties between pirates and the Somali civilian population, with pirate recruitment from among Somali citizens being easy due to poverty and lack of state authority. Moreover, some of the Somali media consider piracy as an act of heroism and see pirates as the defenders of Somali waters against illegal fishing and the dumping of toxic waste into Somali waters.

The Gulf of Aden is transited by over 22,000 commercial ships annually to or from the Suez Canal through the Red Sea and it is the terminal point to the Indian Ocean. Statistically 15% of world oil production and 20% of world trade transits the Gulf of Aden, 80% of total commercial traffic involving Europe. (Roger Middleton, 2008, p.6).

The unconventional actions carried out by Somali pirates in the Horn of Africa have a major economic and security impact. From an economic point of view, the diversion of commercial ships to the Cape of Good Hope involves bypassing the African continent, this route being 2,700 nautical miles longer, which implies additional costs with immediate consequences that will be borne by consumers. We cannot rule out potential marine oil pollution as a result of pirate attacks that would have serious consequences for the environment and the ocean fishing industry.

In order to prevent and deter piracy in the Gulf of Aden, a series of recommendations and measures were adopted for commercial ships transiting this maritime area, as well as the deployment of military capabilities by international bodies such as NATO (North Atlantic Treaty Organization North) and the EU (European Union) by initiating anti-piracy operations to ensure freedom of navigation for commercial ships. A multinational Combined Task Force 151 (CTF 151) was also created to integrate the effort against piracy and other non-NATO countries. CTF 151 is a multinational task force comprising ships from the United States, Bahrain, Brazil, Denmark, New Zealand, Japan, Jordan, Kuwait, Pakistan, Singapore, Thailand, Turkey, United Kingdom with rotational command from 3 months to 6 months from within the contributing nations. (Combined Maritime Forces – CTF-151). CTF 151 has the mission of combating piracy outside the territorial waters of coastal states in coordination with ships participating in the EUNAVFOR ATALANTA anti-piracy operation initiated by the European Union. Other missions of CTF 151 include combating human trafficking and illegal fishing, gathering and sharing information with other actors in the area of operations to maintain freedom of navigation.

The reduction in the number of attacks can be attributed to new proactive tactics adopted by naval groups that resulted in the destruction of pirate boats, thus diminishing the pirates' material resources. (Lucian Valeriu Scipanov, Valentin Marian Toma, 2018, p.162).

It can be concluded that Somali piracy has undoubtedly adapted its tactics to the circumstances, while naval forces have increased their ability to capture pirates and shipping has more possibilities to avoid pirates.

II. Attacks by Houthi rebels in the Red Sea the beginning of a possible regional war

The Red Sea is one of the most important international routes in the world, it is an essential waterway for the transport of goods from the Mediterranean Sea to the Indian Ocean which since November 2023 has become an unsafe maritime space for navigation due to Houthi rebel attacks on merchant ships. Houthi forces in Yemen have begun launching a series of attacks using drones and missiles against commercial and military ships in the Red Sea in response to Israel's ongoing war in Gaza.

In order to have an answer to the question: "What prompted the Houthi rebels to act like this?" Certain events that took place in Yemen, in which the Houthi movement was involved, must be highlighted. The Houthi movement is an Islamic fundamentalist movement in northern Yemen that has opposed foreign influence over the Yemeni government.

In 2015, Iran-backed Houthi rebels took control of the capital Sanaa, and other major cities. Yemeni government forces, backed by a coalition led by Saudi Arabia, have been fighting Houthi rebels, sparking a security crisis in the region. In June 2018 the Saudi-led coalition advanced on the port city of Hodeidah to force Houthi leaders to negotiate a peace deal favorable to the coalition. The strategic importance of the port, given the entry of humanitarian aid to Yemen, led the United Nations to intervene and brokered a ceasefire agreement (Adam Zeidan, Britannica, 2024). Houthi ties to Iran were evident in September 2019, when Iranian-backed Houthi rebels claimed an attack on oil processing facilities in Saudi Arabia. After the events of October 7, 2023, when the Hamas military organization in the Gaza Strip executed a massive attack on the State of Israel prompting Israel to launch a war against Hamas in the Gaza Strip. Houthi rebels with anti-Israel ideology started launching drones and missiles towards Israel and attacking ships passing through the Bab el-Mandeb Strait. Houthi leaders initially said navigation in the Red Sea would remain safe for all commercial ships except those bound for Israeli ports. From November 2023 to January 2024, Houthi rebels launched more than 25 missile and drone attacks on merchant ships transiting the Red Sea and the Gulf of Aden, most of which were intercepted by US naval forces (Adrian Ardelean, Europa Libera Romania, 2024).

The Houthi's main unconventional actions are increasingly based on attacks against maritime targets in the Red Sea in the Yemeni coastal areas they control. The first major weapon that the Houthi rebels have used effectively against warships in the Red Sea is the anti-ship cruise missile (ASCM) and other anti-ship missiles and missiles.

Houthi attacks have disrupted shipping in the Red Sea, causing many shipping companies to abandon the shipping route through the Red Sea and the Suez Canal to the Indian Ocean in favor of a longer one (as previously mentioned and in the case of Somali pirate attacks a detour of 2,700 nautical miles) and expensive around the African continent via the Cape of Good Hope. The redirection of ships to the Cape of Good Hope implies an extension of the transit with an estimated period of between 10 and 14 days, which implies an increase in transport rates and marine insurance. Rising freight costs can lead to a crisis in consumer goods, a disruption in global supply, and rising inflation. (Economica.net, AGEPRES, 2024).

As with the actions of pirates in the Gulf of Aden, almost two months after attacks on merchant ships in the Red Sea by Houthi rebels, efforts have been made to improve the security environment in the region. The United States of America has announced an initiative to protect commercial traffic by launching Operation Prosperity Guardian, a multinational operation to ensure freedom of navigation for commercial vessels transiting the Red Sea. Amid continuing attacks on shipping, US and British forces in the region have launched a series of attacks on targets in Yemen in order to reduce the fighting capacity of the Houthi rebels.

The new security context in the eastern Mediterranean where Israel continues its bombing campaign against Hamas in the Gaza Strip, the firefights in northern Israel between Israeli forces and the Iran-backed Hezbollah organization in Lebanon, plus the crisis caused by attacks by Houthi rebels in The Red Sea could be the reason for a substantial military presence in the region.

I believe that based on religious or economic criteria, hostilities can quickly escalate into a war in the region with coalition implications, a fact that would lead to the establishment of navigation conditions in the Red Sea. In this case, the economic interests of China and the Russian Federation in the region may be affected. By affecting the economic interests of China and the Russian Federation, it is possible that the tensions between these countries will increase, constituting a potential danger to international peace and security.

III. Drifting mines in the Black Sea danger to freedom of navigation

The Russian Federation's aggression against Ukraine has turned the northern Black Sea into a battleground for the exercise of sea control. The concept of sea control involves maintaining freedom of navigation for one's own or neutral merchant ships and cutting off an adversary's sea lines of communication. Maritime communications mean "*ports and navigable routes between ports with specific navigation facilities and transport ships using these routes*"(Marius Hanganu, 1998, p.194). In the case of the war between the Russian Federation and Ukraine, comparing the number of forces and naval means of the two countries, the balance clearly tilts in favor of the Russian Federation, but the control of the sea initially obtained by the Russian Federation is strongly contested by Ukraine through the successful use of autonomous systems without pilot and surface-to-ship missiles against Russian military vessels. In order to prohibit the access of military ships in certain directions, Ukraine and the Russian Federation have planted mine dams along the coast thus restricting the freedom of navigation. The greatest threat to ships sailing in the Black Sea is drifting mines that have been dislodged from mine barrages due to adverse weather conditions or have been intentionally launched by one of the two parties in order to create a mine hazard and determine one of the parties to withdraw their naval forces in ports. There are suspicions that Russian ships have launched drift mines to limit and even prohibit commercial traffic in the western Black Sea, Ukraine being one of the world's main grain exporters (Colectiv, 2023, p.4). The main beneficiaries of Ukrainian agricultural products are countries in Africa, Asia, and the Middle East. Since the beginning of the Russian invasion of Ukraine in February 2022, Ukrainian agricultural exports have been severely affected by the four-month blockade by Russian Federation military vessels of Ukrainian Black Sea ports.

Between July 2022 and July 2023, there was an agreement between the United Nations, Turkey, and Russia (the Black Sea Grain Initiative) to create a humanitarian corridor through which Ukrainian grain would be transported. On July 17, 2023, Russia announced its decision to no longer allow the export of Ukrainian grain. Through the concluded agreement, Ukraine exported more than 33 million tons of grain and other food products. Through the United

Nations World Food Program (WFP) alone, during the implementation of the initiative, more than 725,000 tons of wheat were shipped from Ukrainian ports and transported to Ethiopia, Yemen, Sudan, Somalia, Kenya, and Djibouti (European Council, Black Sea Grain Initiative, 2023).

After the announcement of the decision of the Russian Federation to abandon the continuation of the agreement for the export of grain by Ukraine, Romania became the main export route for Ukraine. The maritime and Danube ports are very crowded, with many commercial ships anchored at sea near the Romanian shore, waiting to be loaded with agricultural products. These ships are exposed to the danger of mines when they are stationed in harbors and when they are sailing on trade routes. Throughout the conflict, several commercial ships hit drifting mines, the material damage being particularly significant. A major threat to the Black Sea ecosystem is oil pollution resulting from the serious damage or sinking of commercial vessels carrying petroleum products and hitting a drifting mine.

Drift mines are generally small in size and are designed to explode in contact with a ship's hull. As weapons, they are relatively cheap and can be launched from many types of ships, not just specialized ships. They are difficult to detect with onboard reconnaissance, especially at night. Most of the time to be sure of the identification of a sea mine it is necessary that the sea mine be visualized because many objects floating on the sea can be mistaken for drift mines.

Drifting mines are extraordinarily difficult for the Navy to counter because most of the mines' countermeasures capabilities are designed to counter fixed minefields. A traditional way of countering drifting mines involves sailors standing watch, and scanning the waters around the ship. When it detects a nearby mine, the ship may turn to avoid it, use a water cannon to push it away or attempt to sink or detonate it with gunfire. However, it's hard to spot a dark, semi-submerged object – especially at night, in fog or rough seas.

The danger of drift mines influences not only maritime transport but also fishing activities, tourism, extraction, and transportation of hydrocarbons through the effects generated upon impact and the psychological effects produced by the danger of mines.

To reduce the danger posed by drift mines, each country bordering the Black Sea has created its own warning, information, and action system. The Romanian Naval Forces act with specialized forces and means to ensure freedom of navigation in the Black Sea so that the commercial flow can take place at a normal pace.

In order to minimize the risks of mine danger, Romania, Bulgaria, and Turkey concluded, on January 11, 2024, a cooperation agreement for demining the Black Sea, by creating a Mine Countermeasures Task Group. (BucPress, 2024). Following the operational planning process, the Mine Action Group will become operational so that it can operate effectively in its area of responsibility.

Conclusions

Unconventional actions with the effect of limiting and even prohibiting freedom of navigation have a major impact on the global economy, generate financially costly countermeasures for countries that have deployed military forces in hot regions, and can lead to the outbreak of regional conflicts.

Piracy is a threat to the international transport of goods and the stability of the world economy, the presence of legitimate military forces being absolutely necessary to protect commercial ships and ensure freedom of navigation in high-risk areas. The concerted efforts of the NATO and EU Naval Groups, combined with the activities of other international actors have considerably reduced piracy in the Gulf of Aden and off the coast of Somalia.

I believe that for Romania the phenomenon of piracy in the area of the coast of Somalia must be worrying as a member country of the European Union and as a country that has a marine education system that provides personnel for the international maritime industry.

More complicated than what has been stated above is the situation in the Red Sea, where the Houthi rebels are using drones and missiles against commercial ships, and the actions of hitting some Yemeni vessels by American and British forces may lead to the outbreak of a regional conflict on a much wider scale. This claim comes amid Houthi rebels' actions in the Red Sea in response to the war in the Gaza Strip. The strikes executed by the American and British forces can lead to the radicalization of the Houthi leadership and those who support the actions of the rebels with weapons and ammunition systems. This complicated situation puts regional actors in difficult situations, such as Saudi Arabia, which is concerned about possible rebel attacks on oil infrastructure, which is why it prioritizes a peace deal in Yemen. There is also the possibility that amid the escalation of the conflict, it would be possible to strengthen Iranian influence in the region. Economically, shipping costs have increased and an increase in the price of oil is possible, which would lead to an economic crisis of global proportions.

The war between the Russian Federation and Ukraine creates a complicated situation in the Black Sea in terms of commercial trade and the exploitation of natural resources. Using drift mines as a method of interdiction at sea endangers freedom of navigation and maritime trade which creates effects on global food security. Before the invasion of the Russian Federation, Ukraine was the fourth largest grain exporter in the world, with 70% of exports going at sea. Even though Romania has become the main export route for Ukrainian grains, commercial traffic in the Black Sea has been reduced due to the danger of drifting mines and the consequences of explosions generated by commercial ships hitting them.

Upholding freedom of navigation for commercial vessels represents unfettered access to sea lanes to support global economic development, actions to limit freedom of navigation being a threat to the legal foundation of international law.

BIBLIOGRAPHY:

1. (Adrian Filip, 2013, p.113) Filip, Adrian. Teoria relațiilor internaționale, Puterea maritimă la început de secol XXI. Editura SINTECH, Craiova, 2014.
2. (Teodor Frunzeti, 2013, p.8). Frunzeti, Teodor, Straregic Impact Strategic, București, 2013.
3. (Marius Hanganu, 1998, p.194). Hanganu, Marius. Apărarea comunicaţiilor maritime de către forţele flotei maritime în condiţiile geopolitice actuale, în Gândirea militară românească, nr.1/1998.
4. (Roger Middleton, 2008, p.6) Middleton, Roger. Piracy in Somalia, Threatening global trade, feeding local wars, Chatham House, Briefing Paper, Africa Programme (October 2008).
5. (Colectiv, 2023, p.4) Seth Cropsey, George Scutaru, Harry Halem, Lairențiu Pachiu, The Battle for Black Sea! The Importance of Freedom of Navigation and Energy Stakes, New Strategy Center, 2023.
6. (Lucian Valeriu Scipanov, Valentin – Marian Toma, 2018, p.162) Lucian Valeriu Scipanov, Valentin-Marian Toma, PIRATERIA între mit și realitate, Editura Universității Naționale de Apărare “Carol I”, București, 2018.
7. (Geoffrey Till, 2013, p.33) Till, Geoffrey. A Guide for the Twenty-first Century, 3 rd ed., Routledge, London and New York, 2013.
8. (Adam Zeidan, Britanica, 2024) https://www.britannica.com/topic/Houthi-insurgency-in-Yemen.
9. (BucPress, 2024) https://bucpress.eu/turcia-bulgaria-si-romania-au-semnat-un-acord-privind-deminarea-marii-negre.

10. (Combined Maritime Forces – CTF-151) https://combinedmaritimeforces.com/ctf-151-counter-piracy/.
11. (European Council, Black Sea Grain Initiative, 2023) https://www.consilium.europa.eu/en/infographics/ukrainian-grain-exports-explained.
12. (Economica.net, AGEPRES, 2024) https://www.economica.net/conflictul-din-marea-rosie-nu-inseamna-o-noua-criza-a-lanturilor-de-aprovizionare-analiza_720406.html.
13. (The Journal of Economic Perspectives, Vol.33, 2019) https://www.jstor.org/stable/resrep02475.8.
14. (Adrian Ardelean, Europa Libera Romania, 2024) https://romania.europalibera.org/ a/cine-sunt-rebelii-houthi/32771644.html
15. (Seaman, 2018) https://seaman.ro/shipmap-vizualizare-incredibila-a-traficului-naval-global/
16. (Small Arms Survey, Somali Piracy, 2012, p.197) https://www.smallarmssurvey.org/sites/default/files/resources/Small-Arms-Survey-2012-Chapter-06-EN.pdf
17. (UNCLOS, United Nations, p.53) http://www.un.org/Depts/los/convention_agreements/texts/uncl

1053477-3045-1396-24-33

HISTORY OF THE MOUNTAIN TROOPS
– FROM NECESSITY TO ESTABLISHMENT –

Cristian - Octavian STANCIU, PhD.
Colonel, Associate professor, PhD., ”Carol I” National Defence University,
Bucharest, Romania
E-mail: cristianstanciu73@yahoo.com

Cristian - Tiberiu CRISTESCU, PhD. candidate
Colonel, 2nd Mountain Brigade „Sarmizegetusa”,
Brașov, Romania
E-mail: ccristi2577@yahoo.com

Abstract**:** *"The need to defend the country in order to preserve its territorial integrity, combined with the geopolitical situation in the 19th century, led the decision-makers of that time to rethink the organization and equipping needs of the army. The predominantly mountainous terrain in the central area gave rise to the idea of setting up special troops to operate in the Alpine environment – the mountain troops. "*

Keywords**:** *Romanian Army, mountain troops, treaty, military campaigns, establishment*

Introduction

The Alpine area needs to be covered during military actions at this level by specialized forces, by the military structure capable of carrying out combat missions within military operations, by the military structure capable of survival and independent actions, with self-support, in this area. These military structures are the mountain troops, whose actions are mainly carried out in the alpine environment and against an adversary prepared to act in the same action environment. They are the most effective and most of the time reach effectiveness as well as the level of preparation and due to the capabilities for which they are developed. However, it is necessary to understand that certain principles of combat such as effort capacity, maneuver, economy of forces and means, speed, and surprise of the enemy can significantly tilt the balance in favor of those who respect them and can apply them.

The emergence of distinct specializations within the armies of different nations, proof of which is the history of European mountaineers and mountain troops, presented the appropriate opportunity for the establishment of mountain troops in the Romanian army. The need to defend the country in order to preserve its territorial integrity, together with the geopolitical situation of the 19th century, led the decision-makers to rethink the organization and equipment of the army.

Due to the geographical characteristics of Romania, predominantly mountainous in the central area, the idea of setting up a specialized corps of troops to operate in the mountain operational environment was born.

It was discovered that the alpine areas need to be protected by specialized forces, and military units capable of surviving and independent self-sustaining actions. These military units are mountain troops, whose actions are predominantly carried out in the alpine environment and against an adversary prepared to act in the same environment. They are efficient and effective because of their specialized training and the capabilities they can employ. It is necessary to understand, however, that certain principles of combat such as effort, maneuver, the economy of force and means, speed, and surprising of the enemy can tip the balance significantly in favor of those who respect and appropriately apply them.

Long-term resilience and resistance within the mountains, especially in the alpine areas, means achieving the decisive objectives of all operations, stopping, destroying (denying) the aggressor, firmly holding the hard ground, keeping communications and settlements under control, even when the adversary has penetrated deep on some directions.

War has always demanded adaptability, flexibility, and change, regardless of the areas where it takes place or the actors involved. These are some of the most important principles behind the planning and use of troops in combat. Towards the end of the 19th century, Romania needed to reorganize its army in order to better adapt and deal with potential aggressors in mountainous areas.

During the First World War, after the loss of the Carpathian passes and the withdrawal of the Romanian army to the south, the state authorities were warned about the need to create specialized troops, able to carry out combat actions in the mountains, with maneuver capacity and equipment appropriate to this operational environment.

1. Where and how the first mountain troops appeared in Europe

Europe was the first training center for alpine and mountain troops. The first countries to set up such troops were the countries with large, heavy, and extensive mountain ranges, such as Switzerland, Italy, France, Germany, and Austria, all of which had territories within the mountainous areas of the Alps. Initially, these troops were called, ALPINE", having a territorial character. Since the formation of the Swiss Confederation (1848) this country has had mountain companies, which in 1911 were formed into units and large mountain troop units.

The place of honor, however, in the establishment of the first alpine troop units went to Italy in 1872, a country which only after 13 years, in 1885, had six regiments, totaling 20 battalions of alpine troops, a figure which could be increased to 29 battalions and nine regiments during a mobilization. For these units, the principle of recruitment was territorial, by companies, which in combat operated in the region from which they were recruited.

In 1888 France had an Alpine division on the border with Germany, called the Vosges Division, which in turn was made up of battalions of mountain troops, infantry line regiments, and mountain gun batteries. During the same year, France changed the organization of the division to include a variable number of groups, battalions of mountain chasseurs, mountain gun batteries, and a light infantry brigade.

The Austro-Hungarian Empire had the largest and most numerous numbers of mountain troop units, which in 1893 had a Tyrolean mountain regiment called the 2nd Regiment of Tyrolean Imperial Mountain Troops (2 Regiment Der Tiroler Kaiserjager), consisting of 12 battalions of four companies each. Apart from these, Austro-Hungary had 30 independent mountain troops battalions in various mountainous areas of the empire. By the beginning of the First World War, Austro-Hungary had established four Kaiserjager regiments, and in 1915, at the height of the war, it had 16 Alpine brigades, three of which were deployed on the Romanian front in 1916 (2nd, 8th and 10th Brigades), of which the 8th Alpine Brigade on the Zărnești - Rucăr corridor, while the 2nd and 10th on the Turnul Roșu pass.

Germany had some Bavarian and Prussian mountain battalions around the outbreak of the First World War, which together with the Infantry Guards Regiment formed the German Alpine Corps, a large unit that in 1916 was deployed from Verdun to Sibiu, on the Romanian front.

After the end of the Second World War, the interest of the great powers in alpine and mountain troops faded, by their promotion of the offensive military doctrine, with the large-scale use of weapons of mass destruction, a concept adopted by the U.S. and U.S.S.R., being transposed into the practice of troops training by the two opposing military blocs – N.A.T.O. and the Warsaw Treaty. During the whole period of the "Cold War", the prospect of mutual destruction and the establishment of the eternal nuclear night was circulated more and more. The commando subunits, the long-range reconnaissance subunits, the subunits fighting behind the enemy's front, and lately the military actions against terrorism, the most feared modern and contemporary military action, appeared and developed a lot.

Today, the entire system of alpine troops and mountaineers in Europe has been radically changed, restructured, and reorganized, significantly reducing the number of units and large units with a mountain profile, a process completed in 2008. Switzerland has radically restructured its military system, maintaining the organization of mountain hunters in territorial divisions (D.1 – 4 V.M.), and landwehr, which have missions to cover and defend the mountainous area. According to tradition, Italy still actively maintains the 4th Alpine Corps in the mountainous area in the north, which includes a variable number of Alpine brigades and other independent units.

2. The first attempts at establishing the mountain units in the Romanian Army

The brief information on the history of European Alpine and mountain troops provided the premise to appreciate the opportunity of the establishment and the role that the mountain troops had to play in the Romanian military system.

The evolution of the Romanian state after the Unification of 1859 and the gaining of State Independence in 1877, promoted the idea of achieving full national unity and regaining territories lost to the neighboring countries. But the political and military situation in Europe at the end of the 19th century and the beginning of the next was marked by two completely opposed and unresolvable tendencies, on one hand, the desire of the peoples subjugated by Germany, Russia, and Austro-Hungary to complete their national unity and to liberate their brothers under foreign domination, and on the other hand the determination of these dominant empires to perpetuate the status quo and maintain their domination. To this conflict-generating contradiction at home was added another of an external nature: the hardening of the contradictions between the great empires for a new world order divided into spheres of influence, along with their desire to secure their hegemonic positions in Europe and the world.

The signing by King Charles I in 1883 of the Alliance Treaty between the Austro-Hungarian Empire and Germany was intended to bind Romania to these states in order to protect and defend their interests. All three parties considered that Romania would be protected against a possible Russian expansion in the Balkan Peninsula, accepting military aid from these two empires if necessary, in which case Romania was obliged to do the same. As a result, during the period in which this treaty was in force (1883-1914), Romania had to soften or cancel its claims against Austro-Hungary by improving the situation of the Romanians who lived in the provinces under the Empire’s occupation and also accept the border established on the Carpathian mountain range, the disappearance of which should be left to the political game or to more favorable times. Between 1883 and 1914 there was nothing that could be done in order to establish a corps of mountain troops in Romania, given the firm position of the Romanian *"allies"*, who had no interest in having such specialized troops along the Carpathian mountain range.

The treaty was signed in secret on the 30th of October 1883 in Vienna, at the insistence of the King of Romania and the politician I.C. Bratianu, who feared a vehement reaction from the Romanian public opinion. For this reason, the agreement that linked our fate to that of the Central Powers was not even submitted to debate and ratification by the Romanian Parliament, the application of its provisions being dependent only on the King’s whims.

The treaty put an end to the hopes of all Romanians to see specialized troops on the Carpathian mountain range. This dream would only be realized 33 years later, in 1916, when this treaty lost one of its supporters (King Carol I), just as the Romanian War of Reunification began.

Despite these difficulties and obstacles resulting from Romania's membership in the military coalition of the Central Powers, between 1883 and 1914 there was a serious undertaking to improve the Romanian military structures and also to create units of mountain troops. In the beginning, LT Grigorie Bunescu published a study with the title *”,Dorobanții de montate"* in the magazine *”Armata"* in 1889, in which he made a thorough geographical and military analysis of the temporary border imposed on the Carpathians. For the defense of the Carpathians, as well as for the prosecution of offensive operations beyond them, the officer proposed to have prepared in advance a defensive system led by a strong military leadership. In the final part of the study, the officer proposed the organization of the mountain troops, the first step being the subordination of the "Mountain Dorobante Companies" to the "Mountain Dorobante Battalions", which would bear the names of the most important valleys in the area of deployment, proof that these troops had barracks along the most important valleys in the Carpathians.

In 1892, CPT I.D. Topliceanu, in a study entitled *"The necessity of special mountain troops"*, published in the magazine *"România Militară",* presented the advantages of these troops:

- a good knowledge of the area where they had to operate;
- more than sufficient knowledge of the border with the neighboring country;
- the units were drafted from those difficult regions;
- the morale of the defenders being high because the soldiers were supposed to defend their homeland of their families that inhabited those areas.

In 1893, the same officer, Grigore Bunescu, reiterated in a study entitled "*The Organization of the Army*", the idea of organizing the mountain troops into *"mountain troops battalions".*

3. The formation of mountain troops unites in the Romanian Army

The determining factor in the Romanian Army's decision to create the mountain troops on its territory was the unfavorable course of the military campaign in the autumn of 1916. The battles fought by the three armies (North, 2nd, and 1st) on the Carpathian mountain range demonstrated beyond all doubt that the lack of these specialized troops was a serious handicap for Romania.

Based on Order no. 294, issued on the 3rd of November 1916 by Romanian General Staff, the Military Ski School in Bucharest was transformed into the first Mountain Troops Corps, a fighting unit organized into three battalions, each with three companies, all with a strength of 1980 soldiers, under the command of which CPT Virgil Bădulescu. In the same order, it was also stipulated: *"These mountain fighters will be specially trained for mountain warfare, being especially destined for reconnaissance, security, and liaison missions. The soldiers may also be called upon to operate as a tactical unit within the Carpathian passes. A special and permanent corps of mountain troops will be set up under the name of MOUNTAIN HUNTERS".*

On a gloomy autumn day in November 1916, when the German-Austrian-Hungarian armies had invaded Oltenia, Muntenia, and conquered the ridges of the Southern and Curved Carpathians, the mountain troops recruited from the entire army began to gather in the barracks of the 4th Roșiori Regiment in Bucharest's Cotrocenii. In a paper written by MAJ Radu Teodoru, former commander of the 2nd Mountain Company he wrote: "In those autumn days, at the beginning of November, the thin defending lines of our armies, were penetrated while being scattered along the wide borders. Numerous enemy armies rushed up the Jiu Valley, crossing over the whole stretch of proud Oltenia, over the plains, over the villages, overwhelming everything in their path like angry floods. Our armies, without any defense against the enemies that were coming from all sides, had to retreat, more and more backward towards the heart of the country, where they gathered before Bucharest, for a last desperate resistance.

In those days of public grief, with the pain of an entire country, the mountain troops gathered in Bucharest. Every day soldiers arrived from all over the country. In the barracks of the 4th Roșiori Regiment in Cotroceni, soldiers from all the regiments gathered, like school children at the beginning of school. Those first beginnings of the mountain units were sad. There, in the empty, deserted barracks, they lingered for days on end, postponing their departure from one day to the other, waiting with hope for the outcome of the great battle of Argeș, in which the fate of Bucharest, the fate of the country, was at stake".

On the 27th of December 1916, ***the Mountain Troops Corps*** was transformed into the ***Mountain Troops Battalion***, organized into five rifle companies, two machine-gun companies, and a signal section, with a strength of 4,000 fighters. The strength of one company reached 500 soldiers.

Between January and June 1917, the entire Romanian Army, with the help of the French Military Mission in Romania which provided instructors, the mountain troops battalion underwent a rigorous process of reorganization, equipping, and training following a new combat doctrine, an action rarely seen in universal military practice. The new combat doctrine consisted of replacing the frontal attack, in which compact masses of men took part, with the application of the trinomial **"*fire*, *movement, strike*",** a practice that persists in the Romanian Army even today. The concept of resizing the Romanian Army consisted of organizing a smaller number of robust units, equipped with modern artillery, machine guns, and automatic weapons in order to overcome the power of the German and Austro-Hungarian divisions, to which were added their own material and medical insurance units, able to give them independence in carrying out combat missions.

After six months of intense training in July 1917, the Mountain Troops Battalion from Tg. Neamț, commanded by MAJ Virgil Bădulescu, presented itself as a properly trained tactical unit, well equipped with weapons, supplies, and horses, able to carry out combat actions in mountainous - wooded terrain. The whole battalion was determined to face the enemy, and such determination could only spring from the surety of being a strong unit, able to face any situation that might arise on the battlefield.

The Great Union proclaimed in Alba-Iulia on December 1st, 1918, by the will of the entire Romanian people and the entry into the composition of the new state of the largest part of the Carpathian Mountains, as well as the whole of Transylvania, determined the increase in the spatial and numerical extent of the mountain troops.

The process of expansion of the mountain hunters started from the bottom up, favored by the existence at the command of R. 8 V.M. of Lieutenant Colonel Carol, the Prince of Romania, who through his power directly addressed the General Staff, proposing a new organization of the mountain troops into a special group. Nothing more, nothing less, it was proposed to set up some mixed brigades of hunters of mountains, so that each army corps that has mountains in its territory of responsibility, has a special mountain group. In the proposals presented, it was stated that the project does not solve the entire problem of the organization of mountain troops and that it should constitute a special object of study, directly related to the general organization of the army.

According to the high Decree no. 1674, from July 1st, 1923, the Command of the Mountain Troops received the name of the Corps of Mountain Troops, to whose honorary command the Crown Prince Carol was named. Based on the same decree, the 2nd Mountain

Division from Oradea was named the 2nd Mountain Division, and its command was redeployed to the town of Bistrita. On this occasion, two brigade commands were established, both located in the city of Bistriţa (2nd Mountain Troops Brigade and 2nd Mountain Artillery Brigade).

In 1939, 23 years after its establishment, from one mountain battalion, the Romanian Army came to count 4 mixed mountain brigades with 24 mountain battalions, 8 mountain artillery divisions, and 4 mountain howitzer divisions, a group of mounted scouts, 5 mountain pioneer battalions and a communication battalion.

In 1945, on January 22, the Training Center for Mountain Troops in Predeal was abolished. On May 21, 1945, the Mountain Corps Command and the 4th V.M. Division were abolished. 1st Mountain Division was subordinated to the 7th Army Corps, and the 2nd-3rd Mountain Divisions of the 6th Army Corps, from Cluj. On August 20, 1945, the 3rd Mountain Division was abolished. The 5th, 12th, and 21st Mountain Battalions were transferred to the 2nd Mountain Division, and the 6th, 11th, and 22nd Mountain Battalions became part of the 1st V.M. Division, each division having three groups of three battalions each, deployed as follows:

- Group 1 Mountain in Braşov (2nd, 3rd and 23rd Mountain Battalions);
- Group 11 Mountain at Predeal (1, 4, 24 MountainBattalions);
- Group 12 Mountain at Târgu Mureş (6, 11 and 22 Mountain Battalions).

The 2nd Mountain Division had the groups deployed as follows:

- Group 5 Mountain at Sighet (8, 9 and 10 Mountain Battalions);
- Group 7 Mountain in Bistrita (7, 15 and 16 Mountain Battalions);
- Group 6 Mountain in Cluj (5, 12 and 21 Mountain Battalions).

On 14 April 1961, the mountain troops were completely eliminated by disbanding the last existing formation, the 2nd Mountain Brigade. Then, on April 14, 1961, the last military mountaineer from the Romanian Army disappeared, a sad and difficult moment for current and future generations to understand. However, it was re-established on October 14, 1964, from the Order of the MFA, the first mountain unit being the 2nd Mountain Brigade. Initially, the brigade was based in Baia Mare, but on November 1, 1964, the headquarters was moved to Brașov. In the following five years, the 1st VM Bistrita, 4th VM Curtea de Argeș, and 5th VM Alba-Iulia brigades were also established.

After the 1989 Revolution, the 7th Petroșani Mountain Brigade and the 61st Mountain Hunters Brigade were established. Following reorganizations, only the 2nd Mountain Brigade and the 61st Mountain Hunter Brigade are currently active.

Conclusions

Regardless of the doctrines adopted, the political and military leaders of the various European states could not fail to consider the mountainous geographical area as a determining factor in the conduct of military operations. The result of this analysis refers to the idea that acting only in "*convenient*" areas will not meet the objectives of large-scale military actions, in which states with armies of millions of men could be deployed. Geopolitical considerations made it clear that all theatres of military actions should include all forms of European topography, including the many mountainous areas with considerable political, military, and economic influence, which could be used as tactical, operational, or strategic defensive lines, for concentrating and launching offensive actions, concentrating supplies, technical and human resources, or for carrying out large-scale maneuvers and liaison operations.

The mountainous areas in the European theatre of military actions, the increase in spatial and temporal military actions and their convergence into all types of environments, alongside the development and emergence of conflict zones in mountainous areas, have made it possible and necessary to create specialized, organized, equipped and trained troops under the requirements of mountain warfare.

BIBLIOGRAPHY:

1. România în anii Primului Război Mondial, Vol. I, 1987, București, Editura Militară;
2. Col. (ret) Gh. Suman, V. Pricop, and Marun Zaharia, 1992, Epopeea Vânătorilor de Munte, București, Editura Militară;
3. Col (rtg) Gh. Suman, and lt.col. C. Cristescu, 2018, Epopeea Predealului în Războiul de Întregire a Neamului, Editura Univers Ştiinţific;
4. Istoria Bg. (D) 2 V.M., 2003, Editura Pro-Transilvania.

1053477-3045-1396-24-34

AGILE COMBAT EMPLOYMENT: A PARADIGM SHIFT IN MODERN WARFARE

Ioana-Iulia MARCU
Major, Command and Staff College, "Carol I" National Defense University,
Bucharest, Romania
E-mail: ioanaiulia.marcu@gmail.com

Bogdan-Mihai IVAN
Captain, Command and Staff College, "Carol I" National Defense University,
Bucharest, Romania

***Abstract**: Agile Combat Employment (ACE) is a transformative concept in modern warfare that aims to enhance operational flexibility, resilience and effectiveness in military activities. This paper explores the key principles, benefits, and challenges associated with ACE, analyzing its potential in adapting to evolving threats and achieving mission success in highly contested environments. By fostering decentralized decision-making, prioritizing mobility, and optimizing multi-domain operations, ACE provides a framework that lays the foundation for responsive and adaptable military forces. Despite its inherent advantages, however, implementing ACE requires overcoming various logistical, doctrinal, and cultural barriers. By delving into pertinent case studies and best practices, the paper offers insights into how militaries can effectively integrate ACE into their operational practices, ultimately shaping the future of warfare.*

***Keywords:** agile, employment, capabilities, airpower, operations.*

Introduction

The landscape of modern warfare is characterized by rapid technological advancements and the emergence of new, multifaceted threats. In this era of unpredictable and fluid conflict scenarios, conventional military strategies have encountered limitations, prompting a significant reevaluation of operational doctrines. One such response to the evolving theater of war is the concept of Agile Combat Employment (ACE), a strategy born out of necessity to inject adaptability and resilience into military operations.

ACE marks a departure from traditional, rigid force structures towards a more dynamic, flexible approach. As a paradigm shift, it signifies the critical transition from large, centralized bases to a network of dispersed, agile forces capable of rapid response and sustained operations across multiple domains. This radical transformation is designed to enhance survivability while complicating the calculus of adversaries attempting to target or outmaneuver coalition forces.

This paper embarks on a comprehensive exploration on ACE, dissecting its inception as a transformative military strategy, examining its applications in various case studies and considering its future implications for global defense.

1. Conceptual Framework of ACE

Agile Combat Employment is defined by Air Force Doctrine as a "proactive and reactive operational scheme of maneuver, executed within threat timelines to increase survivability while generating combat power" (US Air Force Doctrine Note1-21, 2).

This concept can be traced back to the evolving nature of global conflict zones and the changing dynamics of military threats. Considering the guerilla warfare tactics, mobile operations Anti-Access/Area Denial (A2/AD) capabilities, cyber warfare and asymmetric operations, traditional, centralized, and large-scale military bases have become increasingly vulnerable to sophisticated enemy surveillance and long-range precision strikes. ACE emerged as a response to these vulnerabilities, offering a nimble and adaptive framework for conducting military operations.

Agile Combat Employment is built on several foundational principles that differentiate it from traditional deployment and operational strategies. These principles include (AIRCOM PAO, 2023):

Agility: ACE emphasizes rapid deployment and high mobility. The agility allows forces to respond swiftly to evolving threats and operational requirements, ensuring a dynamic presence across different theatres of conflict.

Interoperability: Interoperability with allied forces and joint operations is a cornerstone of ACE. By harmonizing procedures and technologies among partner nations, ACE fosters a cohesive and formidable coalition response to threats.

Survivability: Mainly to survive the attack of the enemy through dynamic basing and also physical protection of air bases.

Continuity of air-operations: Air activity and the conduct of the air campaign should be maintained without interruption to ensure their effectiveness and to meet the objectives.

Operational readiness: Maintaining readiness for immediate ACE operations to counter any adversary threats swiftly and effectively, with minimal warning.

The strategic objectives of ACE are to enhance force resilience, deter aggression through operational unpredictability and ensure military effectiveness in contested environments.

By adopting ACE, forces can achieve several key benefits:

Enhanced Resilience: by diversifying locations and capabilities, ACE enhances the resilience of airpower. It reduces the operational impact of any single point of failure and allows for sustained operations even in contested environments.

Deterrence through Unpredictability: The unpredictable nature of dispersed and agile operations serves as a deterrent to adversaries. The difficulty in anticipating the movement and actions of ACE forces complicates enemy planning and decision-making.

Cost-Effectiveness: ACE potentially offers cost-effectiveness by optimizing resource utilization. Smaller, more agile units require fewer resources for maintenance and can adapt to various operational needs with minimal additional investment.

Although the benefits are obvious, implementing Agile Combat Employment (ACE) presents a range of challenges, both logistical and strategic, that military forces must overcome. These challenges stem from the need to adapt traditional force structures, doctrines, and support mechanisms to a concept that demands high levels of mobility, flexibility, and self-sufficiency.

Logistical Challenges

➢ Rapid Deployment: Ensuring rapid deployability of forces, particularly to austere and potentially contested environments, requires significant logistical planning and capability development.

➢ Sustainment: Maintaining the sustainment of dispersed forces, especially in terms of resupplying essential goods and munitions, poses a complex logistical puzzle.

➢ Interoperability: The need for seamless integration with allied and partner forces necessitates advanced interoperability, both in terms of technology and operational doctrine.

Strategic Challenges

- Command and Control (C2): Maintaining effective C2 across dispersed units, often operating in environments with contested or degraded communications, requires innovative solutions and robust contingency planning.
- Force Protection: Ensuring the security of forces operating from austere, forward locations against a backdrop of sophisticated enemy surveillance and strike capabilities demands a reevaluation of force protection measures.
- Training and Readiness: Preparing personnel for the diverse and complex scenarios encountered during ACE operations requires comprehensive, realistic training programs that encompass a wide range of skills and competencies.

To address these challenges, military organizations are investing in several key areas:

- Advanced Logistics and Supply Chain Solutions: Utilizing predictive analytics, AI, and unmanned delivery systems to ensure rapid, reliable resupply and maintenance support.
- Robust Communications Networks: Developing and deploying secure, resilient communications systems that can support dispersed operations even in contested electromagnetic environments.
- Innovative Training Programs: Implementing immersive, scenario-based training exercises that simulate the complexities of ACE operations, including joint and multinational exercises to enhance interoperability.

2. Training and Readiness

The successful implementation of Agile Combat Employment (ACE) hinges not only on the conceptual adaptation of military strategy but also on the comprehensive training and readiness of personnel. This section explores the pivotal role of training programs tailored to ACE, the initiatives aimed at enhancing readiness, and the impact of national and international exercises designed to test and refine ACE capabilities.

Training for ACE operations goes beyond traditional military drills and exercises, emphasizing a multi-disciplinary approach that encompasses logistics, communication, rapid deployment, and interoperability skills. Specialized training programs are essential for preparing personnel to operate effectively in dispersed, austere environments with limited support structures:

- Multi-Domain Operations Training: Preparing forces to operate in and across multiple domains—air, land, sea, cyber, and space—ensuring seamless coordination and maximized combat effectiveness.
- Survivability Skills: Focusing on individual and unit-level training on survival, evasion, resistance, and escape (SERE) techniques, critical for operating behind enemy lines or in contested areas.
- Rapid Deployment and Mobility: Enhancing the ability of units to quickly mobilize, deploy, and establish operations in unfamiliar and potentially hostile environments.

Readiness for ACE involves not only the physical and technical preparedness of the forces but also the mental and strategic agility to adapt to rapidly changing scenarios.

Various initiatives and exercises play a crucial role in achieving and maintaining this readiness:

- Agile Flag Exercises: These exercises are designed to test the capabilities of air and ground units to deploy quickly and establish forward operating bases with minimal prior notice, emphasizing the ACE principles of flexibility and mobility.
- Joint and Combined Exercises: Engaging in joint (between different branches of a nation's armed forces) and combined (involving multiple nations) exercises helps to improve interoperability and collective response capabilities under the ACE framework.

2.1 Case Studies and Applications

Agile Combat Employment (ACE) has been applied in various contexts, demonstrating its versatility and effectiveness as a military strategy. This section delves into detailed case studies and real-world applications of ACE, offering insights into its implementation, the challenges encountered, and the lessons learned from these experiences.

Case Study 1: Operation Inherent Resolve

In Operation Inherent Resolve, the campaign against ISIS in Syria and Iraq, ACE principles were utilized to enhance the flexibility and resilience of coalition forces. Operating from dispersed locations, forces were able to maintain a sustained air campaign against ISIS targets, adapting quickly to the dynamic battlefield environment. This operation showcased the importance of rapid deployment capabilities, logistical self-sufficiency, and the ability to operate effectively in austere conditions.

Challenges: Navigating complex political landscapes, ensuring the security of forward-operating bases, and maintaining supply lines in a highly contested environment.

Lessons Learned: The critical role of local partnerships, the need for robust intelligence and surveillance capabilities, and the effectiveness of a decentralized command structure.

Case Study 2: Pacific Deterrence Initiative

Under the Pacific Deterrence Initiative, the U.S. and its allies have been enhancing their presence and capabilities in the Indo-Pacific region to counter strategic competitors. ACE principles are central to this effort, with an emphasis on dispersing forces across the vast region to enhance survivability and operational reach. Exercises and deployments have focused on rapid mobility, logistics innovation, and interoperability with regional partners.

Challenges: Overcoming logistical hurdles across vast distances, ensuring effective communication in a dispersed force structure, and integrating operations with allies and partners.

Lessons Learned: The value of pre-positioning equipment and supplies, the necessity of advanced logistical planning tools, and the benefits of joint and combined exercises to enhance interoperability.

Case Study 3: Enhanced Forward Presence in Europe

NATO’s Enhanced Forward Presence in Eastern Europe serves as another example of ACE principles in action, aimed at deterring aggression and ensuring the readiness of forces. By deploying multinational battle groups in a forward but dispersed manner, NATO has increased its ability to respond rapidly to potential threats while complicating adversarial planning efforts.

Challenges: Balancing deterrence objectives with political sensitivities, maintaining the readiness and cohesion of multinational units, and ensuring robust C2 structures.

Lessons Learned: The importance of continuous, realistic training exercises, the effectiveness of a unified but flexible command structure, and the critical role of local infrastructure and support.

Case study 4: Baltic Region Air Policing

NATO employs ACE in its air policing mission over the Baltic states, where quick-reaction alert interceptors must be ready to scramble at a moment’s notice. The ability to operate from various locations with a minimal footprint epitomizes the ACE concept in a practice constrained by the region’s geopolitical sensitivities.

Challenges: Geopolitical sensitivity, logistical complexity and the requirement of high interoperability standards among the different NATO countries.

Lessons Learned: Detailed pre-planning and having contingencies in place can mitigate the complexities of rapid deployment and also that harmonizing procedures, communication protocols and equipment across allied forces enhances the effectiveness of operations.

These case studies serve as exemplars of ACE's practicality and versatility in various operational terrain and threat environments.

3. Future of ACE

The future of Agile Combat Employment is marked by continuous innovation and adaptation. As technological advancements redefine the art of the possible, ACE offers a framework that capitalizes on these developments to enhance military flexibility, resilience, and strategic depth. The integration of AI, unmanned systems, cyber and space capabilities, alongside a commitment to multi-domain operations, international collaboration, and adaptive training, ensures that ACE remains at the forefront of modern military strategy.

3.1 Technological Innovations Shaping ACE

The integration of emerging technologies is set to redefine the operational capabilities underpinning ACE. Artificial Intelligence (AI) and Machine Learning (ML) are at the forefront, offering predictive analytics for logistics and supply chain management, thereby ensuring that dispersed forces remain well-equipped and operationally viable. These technologies also enhance decision-making processes, providing commanders with real-time data and predictive insights that drive faster, more informed operational decisions.

Unmanned Systems and Robotics are another technological frontier revolutionizing ACE. The deployment of unmanned aerial vehicles (UAVs), unmanned ground vehicles (UGVs), and unmanned underwater vehicles (UUVs) in reconnaissance, surveillance, and logistical support roles significantly enhances force projection and sustainability, all while reducing the risk to human personnel. These systems can operate in austere and contested environments, offering persistent surveillance and rapid resupply capabilities that are critical for dispersed operations.

Cyber and Space Capabilities are increasingly integral to ACE, providing command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) support that underpins operational flexibility and domain awareness. The militarization of space and the cyber domain underscores the necessity for ACE frameworks to incorporate robust cyber defense and space-based assets, ensuring secure communications and situational awareness in the face of anti-satellite (ASAT) weapons and cyber-attacks

The future of ACE is inherently linked to the concept of Multi-Domain Operations (MDO), which seeks to seamlessly integrate actions across all domains of warfare to overwhelm adversaries and create multiple dilemmas. ACE's agility and dispersion capabilities are crucial for the success of MDO, enabling forces to rapidly reposition and exploit temporal windows of advantage across domains. The development of interoperable systems and common operational pictures across allied and partner nations further enhances this integration, ensuring a cohesive and coordinated response to threats.

As security challenges become increasingly transnational, the importance of international partnerships and alliances in advancing ACE principles grows. Joint exercises and collaborative research and development projects foster a shared understanding of ACE concepts, enhancing interoperability and collective defense capabilities. These partnerships not only amplify the strategic reach of ACE but also contribute to a more resilient and responsive international security architecture.

The evolution of ACE necessitates a parallel evolution in military training and doctrine. Virtual reality (VR) and augmented reality (AR) technologies are revolutionizing training programs, offering immersive and realistic simulations of ACE operations. These tools enable personnel to experience the complexities of dispersed, multi-domain operations in a controlled environment, enhancing readiness and operational effectiveness.

Doctrine development must also keep pace, integrating lessons learned from operations and exercises to refine ACE concepts. This iterative process ensures that ACE remains responsive to emerging threats and technological advancements, guiding the development of tactics, techniques, and procedures that leverage new capabilities and address evolving challenges.

3.2 ACE in Romania

Romania's approach to modern military operations, akin to Agile Combat Employment (ACE), involves enhancing its air force capabilities and interoperability within NATO frameworks. Though there is not a direct Romanian equivalent of ACE mentioned explicitly in the sources, Romania's recent military developments and collaborations align with the ACE principles of flexibility, survivability, and operational effectiveness.

One significant instance of Romania aligning with ACE principles is seen in its collaboration with NATO's Air Shielding mission. In October 2023, French Rafale fighters joined Romania for ACE operations as part of this mission. This deployment emphasized enhancing the survivability and operational effectiveness of NATO aircraft and systems, showcasing cohesion and interoperability between allied forces, a core aspect of ACE.

Furthermore, Romania's Air Force, over the years, has focused on modernizing its capabilities, aligning with the ACE emphasis on multi-role and responsive air power.

As a NATO member, Romania is involved in collective defense measures, which include interoperability and readiness aligned with ACE principles. Its location provides a forward positioning option for NATO forces to respond to regional threats. This requires Romania to develop capabilities and strategies that are agile and rapidly deployable to deter aggression and reinforce the alliance's Eastern Flank.

In essence, while Romania may not have a named equivalent to Agile Combat Employment, its ongoing efforts in modernizing its air force and participating in NATO missions like the Air Shielding align with the fundamental principles of ACE - enhancing flexibility, survivability, and the ability to operate effectively in a range of scenarios.

Conclusions

In concluding the article on Agile Combat Employment, it is essential to underscore the transformative impact this strategy has on modern warfare. ACE represents a paradigm shift, prioritizing flexibility, responsiveness and a multi-domain approach to military operations. This reorientation stands as a testament to the constantly evolving nature of conflict and the necessity for adaptability in the face of emerging challenges.

ACE has offered armed forces the ability to rapidly redeploy resources, diversify their operational footprint, and create uncertainty for adversaries. This dynamic posture is a critical response to the modern threat landscape characterized by hybrid warfare, rapidly advancing technologies, and peer-level state adversaries.

Despite the significant advantages afforded by ACE, it is not without certain challenges. Implementation requires a cultural shift within military organizations, demands for new training protocols, and the integration of innovative technologies which are resource-intensive. Furthermore, the decentralization inherent in ACE necessitates robust communication networks to maintain command and control across dispersed units.

Looking forward, ACE embodies the agility required for success in the 21st-century battlespace. The continued development and refinement of ACE will rely upon lessons learned from real-world applications and regular exercises simulating the complexities of future conflicts. International collaboration and joint exercises with allies are also paramount in establishing interoperability and enhancing the collective defensive posture aligned with ACE principles.

As military strategies continue to develop in response to the changing nature of global threats, ACE stands out as a critical component in the arsenal of modern militaries. It moves away from the legacy systems of the past and embraces a more agile, resilient approach to conducting operations. By doing so, it ensures that forces are not only prepared to meet current challenges but are also poised to adapt swiftly to the unforeseeable conflicts of the future. The ongoing evolution of Agile Combat Employment will, without doubt, shape the landscape of military strategy for years to come.

BIBLIOGRAPHY:

1. *** US Air Force Doctrine Note 1-21 Agile Combat Employment. 2022.
2. Allied Air Command Public Affairs Office. 2023. Agile Combat Employment- Enhancing NATO's Expeditionary Capability and Resilience. Accessed January 30, 2024. https://ac.nato.int/archive/2023/ACE_symposium_23-2
3. Isaiah, Oppellaar. 2023. Agile Combat Employment The Next Big Thing for NATO Air Power. Accessed January 30, 2024. https://www.japcc.org/wp-content/uploads/JAPCC_J36_Art-08_screen.pdf
4. Luca, Chadwick. 2024. MA Terrorism and Insurgency at University of Leeds. Accessed February 2, 2024. https://www.kcl.ac.uk/the-ace-up-their-sleeves-understanding-nato-agile-combat-employment
5. RAND Corporation. 2023. The Forces We Need Building Multi-Capable Airmen to Enable Agile Combat Employment. Accessed February 02, 2024. https://www.rand.org/pubs/research_reports/RRA1746-1.html
6. Tony, Bauernfeind and Alexus, Grynkewich. 2023. Agile Combat Employment: Are we ready?. Accessed February 02, 2024. https://www.airandspaceforces.com/watch-read-agile-combat-employment-are-we-ready/

1053477-3045-1396-24-35

GENERATION AND DEPLOYMENT OF FORCES PARTICIPATING IN UN PEACEKEEPING OPERATIONS FROM A LOGISTICAL PERSPECTIVE

Gabriela-Florina NICOARĂ, PhD.
Major, Superior Instructor, “Carol I” National Defense University, Bucharest, Romania
E-mail: Nicoara.Gabriela@unap.com

Abstract*: As part of the North Atlantic Alliance, in the context of Romania's strategic partnership with the United States of America, as well as an active participant in Non-Article 5 operations and EU peace operations, the Romanian Army has reaffirmed its position as a credible partner in relation to the structures with which it has deployed missions. At the national level, the Joint Forces Headquarters has the leading role in operations conducted outside the national territory and is the translator of the strategic level concept to the tactical level execution elements. Through its plans, it promotes, above all, the synchronization of operations and the multiplication of efforts through the concept of 'joint' operations. In this context, the Romanian Army has extensive experience in force assessment, transfer of authority from the generator, deployment to theatres of operations, command and control during missions, and facilitating logistic support in a multinational context or through national responsibility alone.*

Over time, Romania has experienced episodes relevant to its preparedness through participation in peacekeeping operations under the aegis of the UN, actions carried out as a materialization of Romanian political concern for peacekeeping and international stability. The geostrategic and geopolitical context specific to the last twenty years has led to a shift of attention from this issue to response measures to counter the effects of threats to security and stability. As a result of focusing the main effort on strengthening the defense of the national territory and putting other aspects related to the promotion of national defense and security policies on the back burner, there is a need to update the whole spectrum of information, both procedural and operational aspects related to the specificities of UN-led operations. One argument in this respect is the transposition of the national political will, in the form of a decision of the Supreme Council of National Defence, to provide forces for participation in UN peacekeeping operations. In this context, the present research aims to highlight the mechanisms of force generation in the UN context and the particularities underlying the logistical provision of forces participating in peacekeeping missions.

Keywords: *operational logistics, force generation, deployment, UN operations, peacekeeping operations*

1. General context

Examples from the international arena demonstrate that peacekeeping operations are not only a contemporary approach in a multinational setting but also one widely accepted by numerous states worldwide. A state's engagement in this form of military endeavor not only enhances its credibility among international partners but also necessitates a thorough understanding and procedural regulation of the core activities in which it will be involved.

Over the years, the Romanian state has participated in various missions under the auspices of the UN, driven by its expressed political will to be a significant contributor to the preservation of international peace and stability. Upon assuming a mission under UN auspices, the Romanian Army will undertake a series of steps to generate and deploy the force structure. All these activities, contingent upon the political decision to participate in the mission, involve understanding the strategic will and translating it into concrete plans and activities. In this sense, an important national role is to generate and deploy the structures participating in the mission, and the issues described by these activities are the focus of this analysis.

2. Methodological aspects

Starting from the identified problem of the need to update and readapt the modus operandi in the generation and deployment of forces participating in UN-led missions, the present approach will aim to clarify the following issues:

- briefly outline the UN mission;
- identification of the number of missions carried out and their budgetary impact from a UN point of view;
- the nomination of the main UN structures/bodies and component departments responsible for generating, operating and deploying forces in mission areas around the world;
- presentation of the main stages/moments in the process of generation/deployment of forces established to participate in a UN mission and highlighting the logistical implications.

By going through these steps, the two major objectives set for this approach, namely to present a process of generation and deployment of forces to participate in a UN mission and to identify the logistical implications, will be achieved.

3. Framework of UN peacekeeping mission

The United Nations was born out of the desire of the governments that took part in drafting its declaration to continue the fight against the Axis powers. On June 26, 1945, representatives of 51 countries signed the UN Charter, a document setting out the main structures and specific procedures. Subsequently, on October 24, 1945, the UN came into being with the ratification of this document by China, France, the Union of Soviet Socialist Republics, the United Kingdom of Great Britain, the United States of America and a large majority of other signatories (Fomerand, 2009). The purpose of this organization is to maintain global peace and security by harmonizing the actions of all nations (UN Charter, 1945). It is the most powerful intergovernmental organization in the world, now numbering 193 member states. The UN headquarters is located in the international territory of New York and contains offices in all areas in Geneva, Nairobi, Vienna, and The Hague.

Structurally, the UN is built on six pillars:

General Assembly: debates major issues and recommends action;

Security Council: authorises economic and military action in various disputes. The Security Council is made up of fifty members, five of whom are permanent members: China, France, the Russian Federation, the United Kingdom and the United States;

Economic and Social Council: sponsor trade and human rights organisation;

Trusteeship Council: controls territories under UN supervision;

UN Secretariat: UN administrator responsible for coordinating the work of all UN agencies;

International Court of Justice: debates matters of international law and is the only institution that is located outside New York, i.e. in The Hague in the Netherlands.

From the UN reports analysed which refer to peacekeeping missions, we conclude the following facts: from 1948 to 2023, 71 UN-led operations have been deployed, with 11 active to date (UNMIK Kosovo, UNMOGIP India and Pakistan, UNFICYP Cyprus, UNDOF Israel and Syria, UNIFIL Lebanon, UNTSO Middle East, MINURSO Western Sahara, UNISFA Abyei Area, UNMISS South Sudan, MINUSCA Central African Republic, MONUSCO Congo) involving a total of 78677 civilian, military, police and volunteer personnel from 121 troop contributing countries. The latest UN budget execution amounted to $6.38 billion.

The UN, as a global peace support organisation, authorises and deploys missions wherever the situation requires, with each of its departments having clearly defined responsibilities for the military, civilian, police and/or peacekeeping operational element, as follows:

The UN Security Council authorizes missions and their mandates, i.e. issues general requirements and force allocation levels for new missions or missions undergoing major changes;

The UN General Assembly authorises the funding of missions, based on Security Council resolutions;

The Peace Operations Department is responsible for planning and coordinating operations of high complexity;

The Department of Operations Support, together with the Department of Mission Support, are responsible for deployment, logistical support and budgeting of operation preparation, force allocation, planning at the operational and tactical level, and conduct of operations;

Host Nation, exercises its own sovereignty, with implications for force deployment and mission conduct. Relations with the host nation are based on the Status of Forces Agreement (SOFA), an agreement negotiated and signed with the UN;

Troop Contributing Countries (TCCs) and Police Contributing Countries (PCCs) are responsible for training and equipping forces with major equipment, as well as supporting forces on mission in accordance with their mandates;

Contractors, if available in the area of operations, may provide goods and services in support of the mission.

Considering the theme, we have set out to analyse, in this article, the key institution for force generation and the conduct of peacekeeping missions in the world is the United Nations Secretariat. It is composed of civilian, military and police personnel and has the role of supporting and implementing the tasks and policies of the UN General Assembly and the three Councils on behalf of all its members.

Within the seven component departments of the UN Secretariat, relevant to the matters of generation, deployment and logistical support of forces participating in missions are:

- Department of Political and Peacebuilding Affairs - DPPA ;
- Department of Peace Operations - DPO ;
- Department of Operational Support– DOS .

The latter department is responsible for integrated operational support in the following areas:

- human resources, medical management and occupational safety and health;
- supply chain management, logistics, procurement, and military capability support;
- operational planning and support for generation, support and withdrawal (including liquidation operations) of UN Secretariat entities;
- UN command and administrative support;
- communications and information technology support.

4. Main steps of the generating and deploying forces. Requirements for operational logistics

From the point of view of the forces participating in the mission, the phases of UN peacekeeping missions can be described as: mission planning, deployment to the mission area, sustainment of the force and redeployment from the mission area to the deployment bases at peace.

In terms of operation planning, force generation takes place after an arduous and lengthy diplomatic and political process, the point of departure being the Security Council resolution.

It sets out the mandate and the level of force allocation. It is a result of numerous diplomatic actions with the host nation, following which the Status of Forces Agreement (SOFA) was signed.

The next step is the drafting by the DPO of the Statement of Force Agreement (SFA), Statement of Unit Requirement (SUR, a document containing mission-specific requirements for each unit in the mission, including tasks, specific capabilities, organisation, major equipment and self-sustainment needs) and Rules of Engagement (ROE) and the identification of nations that can contribute forces to the peacekeeping mission. This stage involves issuing invitations and contacting Member States for the allocation of force packages already made available to the UN through the Peacekeeping Capability Readiness System (PCRS). The PCRS is the UN Secretariat's main tool for tracking and monitoring peacekeeping capabilities, the quality of force packages in line with UN standards, and the resources the Member States are willing and able to make available for participation in future operations.

Following verification of Member States' applications to the mission for which the UN Security Council has issued a resolution, the DPO will liaise with Member States to submit the list of essential equipment, force organisation and TCC/PCC capabilities. Once the Member States' TCC/PCC force configuration matters have been agreed upon, they will conduct UN-organised fact-finding visits to the area of operations, which will be summarised in the combined Field Mission/DPO and TCC/PCC fact-finding report.

The above-described preliminary elements form the basis for the refinement of the organising states and equipment list, which will be sent back to the UN for the negotiation of the Memorandum of Understanding (MOU) by the force contributing Member States (military and/or police) and UNHQ. The negotiation of the MOU is a complex process involving troop-contributing state personnel from the operational, financial, personnel, logistical, legal, etc. areas. From a national point of view, the document is an administrative one, signed, most likely by a waiver granted by the Minister of National Defence, by the force generation category, but it has profound operational implications. Given the institutional and legal experience, whereby the forces participating in the mission are operationally subordinated to the Joint Force Headquarters, our view is that the negotiation of the MOU requires also the participation of specialised personnel (operational and logistic) from this headquarters.

The MOU is a binding agreement that sets out the responsibility and standards for the selection and provision of personnel, major equipment and support services for self-sustainment, both provided by the UN and the Member State, in accordance with General Assembly resolutions. UN-led peacekeeping operations differ fundamentally from NATO operations in financial and logistical terms. While NATO operations generate, equip, furnish and secure logistical flows as a result of various types of OPLAN/OPORD, these being a national responsibility, in UN operations the initial point of force planning is the UN Security Council resolution to solve a peace problem anywhere in the world, with member states choosing whether or not to participate in the mission, the decision to participate being financially remunerated according to strict rules, and logistical support responsibilities being shared between the UN and the troop-contributing nation. Reimbursements for TCC/PCC contributions to peacekeeping operations are based on standard reimbursement rates approved by the General Assembly and detailed in the Contingent Owned Equipment Manual.

MOU negotiations are conducted in New York at UN Headquarters with each detachment participating in the operation, resulting in a memorandum for each detachment/contingent.

As soon as the MOU negotiation is completed, the force deployment planning process takes place, which is fundamentally different from the NATO force deployment process. In the case of NATO forces, the force packages made available carry out their own deployment planning process in which the contributing country is responsible for providing the deployment capabilities and support necessary for its own force to reach its final destination. The Allied Coordination Centre (NATO AMCC) is the senior entity responsible for the coordination and deconfliction of the movement, particularly on the strategic component of the movement, and the JTF Commander is responsible for coordination and deconfliction on the operational component, i.e. within the Joint Operation Area (JOA). In UN operations, the Memorandum of Understanding and Reimbursement Policy Section (MRPS) within the Department of Operational Support (DOS) is responsible for leading negotiations with the TCC/PCC for the conclusion of MOUs for the dislocation/redeployment of the force. The MRPS is the focal point for communication between the Permanent Mission of the contributing Member State and the UN Secretariat on matters related to reimbursement of funds and subsequent amendments to the MOU, where appropriate.

Prior to the deployment of the force, the UN will conduct the pre-deployment visit/inspection of the TCC/PCC in order to assess and initiate directions to the detachment, including in relation to training for the mission. The TCC/PCC has a vital obligation to draw up the operationalisation plan based on the UN force generation manuals. This, as well as the concrete elements achieved, will form the basis of the UN inspection to the contributing nation. As the structure in the national C2 chain, which will subordinate the detachment participating in the mission, in OPCOM, the Joint Force Headquarters has the obligation to know the level of equipment and material required by the UN to be held, on deployment, by the TCC, negotiated in the MOU, as well as the standards required by the UN for equipment and stocks, so that, on the one hand, the deployed mission can achieve its objectives and, on the other hand, the detachment is equipped with the equipment and material as close as possible to the lower standard level. We mention this because, if the detachment proves, in accordance with the above provisions, that it is equipped at least to the minimum level of equipment, in the quality at least required by the standards, then the nation will receive reimbursement for this level to which it has committed itself. In the event that the standards, for certain equipment and/or stocks, or the quality level thereof, are not met at least at the minimum level required, the reimbursement level for these will be 0%. Conversely, if the equipment/stock far exceeds the level of standardisation required by the UN, then the calculated reimbursement will be at the level of standardisation required in the MOU and the manuals, which may be a waste of resources for the generating nation. Joint Force Headquarters, at this stage, has two courses of action it can take:

Either to organise its own assessment process, in accordance with UN requirements, for the detachment it is to take over in OPCOM, verifying, statically, the level of individual equipment, technique and equipment in correspondence with national legislation and UN quantitative and quality standards, the level of stocks and their quality and, from an operational point of view, the level of training achieved, in strict correlation with the requirements for the mission; or participate with delegates, as observers, in the pre-deployment visit by the DPO and DOS representatives of the UN General Secretariat, in which case the CFI is not a pro-active body and cannot make adjustments and corrections, in good time, so as to avoid waste of resources and ensure a timely and appropriate deployment of the force.

Once the pre-deployment inspection process is completed, with the UN's overall assessment that the force is adequately equipped and ready to perform the mission requested by the Security Council, the force generation and manning process is considered complete and deployment can begin. When the UN is responsible for the deployment/redeployment, MOVCON/UN will arrange for the movement of all equipment and associated personnel from the point of departure to the final destination (FD) in the mission area. On deployment and repatriation, because there is an associated movement of equipment by sea or air, personal luggage is limited to 45 kg (0.27 m^3) regardless of the unit's duty time. If the unit is on a twelve-month tour of duty, the additional 55 kg of entitlements must be shipped independently of personnel (together, for example, with equipment and/or CARGO, by sea). During the initial deployment of a detachment, if operationally necessary, the UN may approve (usually by scheduled commercial airlift) a forward detachment of up to 10% of the unit strength. The TCC must submit a written request for this at least 30 days before the requested flight date, providing all relevant passenger details (name, nationality, date of birth, passport number, etc.). For movements into/within/out of a mission's area of operations, the UN is responsible for coordinating all movement control operations. This includes obtaining the necessary permits and authorisations for the movement of equipment from the competent authorities in the host country.

Alternatively, the deployment can be planned and executed by Member States in accordance with the Letter of Assist signed with UNHQ. This option allows the TCC to organise the movement of personnel and/or CARGO to/from the mission area using its own means of transport. Such arrangements/contracting fall under the responsibility of the TCC/PCC, but they are obliged to coordinate their movement activities through the MCS (Movement Coordination Section) and to inform the UN of the sequencing and phasing of the deployment and all other details to ensure that the mission is ready to receive/send the forces, equipment and related CARGO appropriately. For this alternative, the TCC/PCC will be reimbursed for conducting the movement in accordance with the standards set forth in the UN manuals. Specifically, the UN can only reimburse the maximum that it would cost the UN to conduct the movement.

A combination of the two options is also possible, e.g. where the TCC/PCC deploys the precursor/advanced detachment (or forward command element) and the UN deploys the main force. Whichever alternative is chosen by the Member States, they are obliged to provide MOVCON with all documents related to the movement (PAX manifest, Weapon manifest, Dangerous Goods documentation, load lists, etc.).

For a smooth and incident-free deployment, the CFI must endorse the deployment plan drawn up by the TCC in accordance with national regulations. Thus, the headquarters must follow the entire deployment concept, carried out in accordance with the option chosen at the time of signing the MOU, the sufficient allocation of movement and transport resources, from the peacetime deployment barracks to the final destination, the spatial and temporal feasibility of the concept (in terms of the correct and efficient choice of breaks, rest stops, refueling points, border crossing formalities and transit of other states, maintenance measures, etc.), allocation of medical resources on the deployment/redeployment route, protection force, coordination with supporting contact points, sufficient allocation of specific equipment for palletisation and containerisation, ensuring training of staff for the movement itself, command-control and signals used during the movement, reporting procedures, etc.

Overall, generation process and deployment steps can be summarized as follows:

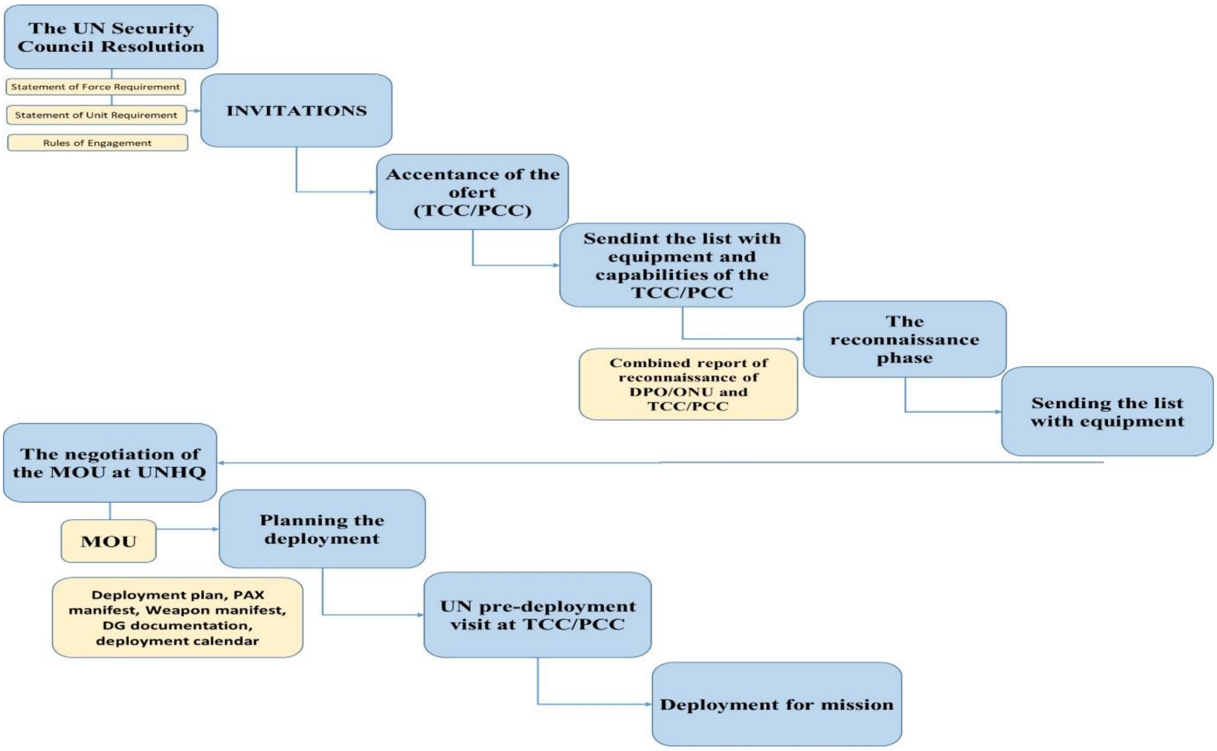

The UN Security Council Resolution
Statement of Force Requirement
Statement of Unit Requirement
Rules of Engagement
INVITATIONS
Accentance of the ofert (TCC/PCC)
Sendint the list with equipment and capabilities of the TCC/PCC
The reconnaissance phase
Combined report of reconnaissance of DPO/ONU and TCC/PCC
Sending the list with equipment
The negotiation of the MOU at UNHQ
MOU
Planning the deployment
Deployment plan, PAX manifest, Weapon manifest, DG documentation, deployment calendar
UN pre-deployment visit at TCC/PCC
Deployment for mission

Figure no. 1: Main steps in generating and deploying forces (source: author)

The force generation process is complex and takes nine to twelve months. The core instrument for the UN to ensure rapid and timely deployment of forces to mission areas is the PCRS, details of which have been provided above. The PCRS is divided into four levels of ambition, of which level 4, the Rapid Deployment Level (RDL), is achieved by the force made available capable of being deployed to the mission area within 60 days of being mandated by the UN Security Council.

Conclusions

The UN operations are primarily conducted for humanitarian purposes and represent an essential instrument in achieving the original objective of the organization. These are and will be necessary, regardless of how the configuration of the global geostrategic situation will appear. At the same time, they represent the military contribution of a long series of convergent actions aimed at contributing to the maintenance of peace worldwide. Romania has experienced peacekeeping missions worldwide. However, the security situation in the Eastern European region and its position at the NATO border compel political-military thinking to allocate resources to secure its own position in the trust architecture built within the alliance. All of these aspects were considered; Romania cannot ignore the international undertaking commitments and the effort that each of us must involve in creating a safer world where the rights of every human being are respected. Whether our country decides to participate with forces in operations under the auspices of the UN or make available forces ready for deployment at a level ranging from 1 to 4, Joint Force Command will have the duty to assess and take under command Romanian contingents equipped and trained to fulfill this type of mission. From this perspective, it is necessary to adapt to the concept of Contingent-owned Equipment (COE), the UN's responsibilities for the logistical components, the logistics responsibilities of nations for the forces sent on missions, UN standards regarding training, equipment, and the criteria and conditions for financial reimbursements.

Overall, we highlight the main documents involved in the process of generating and deploying force:

- The UN Security Council Resolution states the mission, describes its mandate, and establishes the size of the military and police force to be deployed;

- Status of Force Agreement (SOFA) is an arrangement between the UN and the host nation of the mission in which the participating forces are stationed. It establishes the rights and privileges of the foreign military personnel and the equipment and services they benefit from in UN missions.

- Statement of Forces Required (SFR) contains the summary of UN missions, the mandate, the operations concept, capabilities, components, and other requirements of the forces without details for the subunits;

- Statement of Units Required (SUR) contains operational and logistical requirements for each contingent, necessary capability, and other specific requirements;

- Rules of Engagement (ROE) are a set of rules governing engagement with potential enemies and specific situations when the use of force is authorized;

- Verbal Notes are diplomatic papers prepared by the UN but not signed. They represent drafts for the purpose of confirmation by the UN Secretary-General to the nations contributing to missions.

- Reconnaissance reports are written to describe the relevant aspects of the operational and logistical plans of the TCCs/PCCs, which were accepted during the reconnaissance phase.

- Memorandum of Understanding is an agreement between the UN and TCCs/PCCs regarding contributions to UN missions.

These documents must be approached together to prepare forces for UN missions.

BIBLIOGRAPHY:

1. Department of Peace Operations, Department of Operational Support, UN Secretariat, *United Nations Manual for the Generation and Deployment of Military and Formed Police Units to Peace Operations*, May 2021.
2. Jacques Fomerand, *The A to Z of the United Nations*, The Scarecrow Press, Inc. Lanham, UK, 2009.
3. Secretary-General of the UN, *Manual on Policies and Procedures concerning the Reimbursement and Control of Contingent-Owned Equipment of Troop/Police Contributors Participating in Peacekeeping Missions*, 2020.
4. United Nations, Department of Peace Operations, Department of Operational Support, *Authority, Command and Control in United Nations Peacekeeping Operations*, 2021.
5. https://www.mae.ro/node/2114
6. https://peacekeeping.un.org/en/data
7. https://www.un.org/globalcall/content/field-missions
8. https://operationalsupport.un.org/en/background-0

1053477-3045-1396-24-36

IDENTIFICATION OF SOME FUNCTIONAL MODELS OF MARITIME SECURITY STRATEGIES

Iulian-George ANGHEL
master degree student, the Naval Forces Department, the Command and Staff Faculty,
"Carol I" National Defense University, Bucharest, Romania
E-mail: iulian.anghel@navy.ro

Lucian Valeriu SCIPANOV, PhD.
professor eng., the Naval Forces Department, the Command and Staff Faculty,
"Carol I" National Defense University, Bucharest, Romania
E-mail: shcipio@yahoo.com

Abstract: *In the light of the current security environment, especially in the maritime environment, the present paper proposes to carry out an analysis of some maritime security strategies implemented worldwide, highlighting the distinct approaches adopted by various key actors in the field of maritime security. The final goal of this endeavour is to identify some relevant models of maritime security strategies and to analyse the opportunity for Romania to implement an appropriate model of maritime strategy.*

For the complete coverage of the subject addressed, were set the following objectives: the conceptual delimitation of the term strategy from the maritime security point of view, followed by the argumentation of the importance of international and regional cooperation in the maritime domain.

Some examples of states that have implemented a National Maritime Security Strategy and their approach will be used as a working methodology, to identify models of Maritime Security Strategies that can also be adopted at the regional level. Also, the research looks at the adaptability of the maritime strategy in the context of technological progress.

The novelty element of this article consists in the comparative analysis of the various models of Maritime Security Strategies, highlighting the unique aspects and particularities of each, at the same time offering a possible solution for Romania in the situation of initiating the procedures for the development of a national Maritime Security Strategy.

Keywords*: maritime security strategy; maritime security; institutional cooperation.*

Introduction

Given the importance of the maritime domain to the economic development of a state, maritime security has become a critical component of national and allied defense. The importance of ensuring freedom of navigation and free access to maritime resources has determined the rethinking of some solutions for the contribution of state institutions to the consolidation of maritime security, under the conditions of a varied range of threats at sea.

In light of the current security environment, especially in the maritime environment, the present paper proposes to carry out an analysis of some maritime security strategies implemented worldwide, highlighting the distinct approaches adopted by various key actors in the field of maritime security. Thus, models of maritime security strategies implemented at the international level will represent the starting point of the analysis of this paper.

For the complete coverage of the subject addressed, were set the following objectives: the conceptual delimitation of the term strategy from the maritime security point of view, followed by the argumentation of the importance of international and regional cooperation in the maritime domain.

Some examples of states that have implemented a National Maritime Security Strategy and their approach will be used as a working methodology, to identify models of Maritime Security Strategies that can also be adopted at the regional level. Also, the research looks at the adaptability of the maritime strategy in the context of technological progress. This challenge will follow the evolution of disruptive technologies, of the artificial intelligence tool so that the directions of action in the development and implementation of a maritime security strategy capitalize on the benefits of these technologies. However, the primary benefit will be that such a security strategy will also take into account the threats created by these technologies.

The novelty element of this article consists in the comparative analysis of the various models of Maritime Security Strategies, highlighting the unique aspects and particularities of each, at the same time offering a possible solution for Romania in the eventuality of initiating the procedures for the development of a national Maritime Security Strategy.

The final goal of this endeavour is to identify some relevant models of maritime security strategies and to analyse the opportunity for Romania to implement an appropriate maritime strategy model. Once this goal is fulfilled, it will be possible to identify an optimal model of security strategy, the form and the main elements of content, the main guidelines, the necessary means, and the ways of putting it into practice. The problem to be solved will be related to the institutions involved in the development and implementation process of the maritime security strategy.

It started from the premise that in recent times, maritime nations with regional and global interests around the world have recognized the importance of formulating and implementing comprehensive maritime security strategies. This approach explores the current state of implementation of national maritime security strategies, examining key trends, challenges and future perspectives, providing specialists with reasons for reflection and points of departure for further research on the analysed field.

1. Maritime security domain

We begin our endeavour with a conceptual introspection into the field of maritime security and how this issue has become a global and, consequently, a national concern, suggesting that maritime security should be a desideratum at the national level as well.

Globally, concerns regarding maritime security are evident, emphasizing that ensuring maritime security increasingly goes beyond military power and involves the focused attention of relevant organizations in addressing a multitude of challenges, such as piracy, illegal fishing, human trafficking, environmental threats and potential geopolitical tensions. Consequently, maritime security stands as one of the fields benefiting from the latest approaches in international relations.

The main actors in maritime policy, ocean governance and international security have begun, in the last decade, to include maritime security in the discussions agendas or to reorient their activity in such a way that topics from this sphere appear on the negotiating table. To support this observation, some examples can be given:

- The United States of America started this trend in international thinking in 2004, with the introduction of domestic policies addressing maritime security as an additional response to the terrorist attacks in September 2001. Maritime security held a significant place in the American conception due to concerns about maritime terrorism. Despite terrorism not manifesting in maritime dimensions, maritime security remained relevant due to emerging threats in the form of piracy.

- The North Atlantic Treaty Organization (NATO) included maritime security as one of its objectives in the Alliance Maritime Strategy only in 2011. The document, adopted on January 5, 2011, marked the first of its kind in over 25 years and aimed to safeguard the security and prosperity of the allies in the maritime domain[13]. Based on the 2010 Strategic Concept and NATO's three main tasks (collective defense, crisis management and cooperative security), the Alliance's Maritime Strategy in 2011 identified four maritime roles for the Alliance to contribute to: deterrence and collective defense, crisis management, cooperative security and maritime security[14].

- In 2014, the European Union (EU) developed ambitious strategies to enhance maritime security through the European Security Strategy[15]. Through this strategy, the EU established the legal framework and expressed its ambition to take responsibility for security in Europe and other parts of the world.

- Also in 2014, the African Union (AU) developed the African Maritime Security Strategy, representing a commitment to taking responsibility for securing the waters of West Africa[16].

On the same note, civilian stakeholders in the maritime domain reacted as well when the Maritime Safety Committee (MSC) of the International Maritime Organization (IMO) prioritized maritime security on the agenda. Initially fueled by growing concerns about terrorist threats in the naval domain, progress in maritime security emerged alongside the rise of piracy off the coast of Somalia between 2008 and 2011[17]. The threat of piracy for international trade has not only brought the maritime dimension of security into global awareness but has also propelled it high on the political agenda of major actors.

Maritime security may seem like a complex and sometimes unclear concept. In reality, it has become a comprehensive task involving numerous entities from international, public and private sectors, aiming to preserve navigational freedom, facilitate and protect trade and maintain good governance of the seas.

While there is consensus on maritime safety, for which the responsibility lies with the International Maritime Organization (IMO), there is no common definition or consensus regarding the term 'maritime security.' For instance, the IMO amended Chapter XI of the International Convention for the Safety of Life at Sea (SOLAS) with a subordinate chapter, XI-2, addressing maritime security. As a result, it is worth mentioning the ISPS code (International Ship and Port Security)[18], which provides an insight into maritime security. The merit of this regulation lies in introducing the concept of maritime security to civilian decision-makers, establishing a set of guidelines and generating awareness about the need for a more detailed discussion of the issue.

In other words, maritime security is a responsibility that lacks a universal or agreed-upon definition due to its comprehensive nature, covering multiple domains. However, it centres around ideas unanimously accepted by most relevant institutes in the maritime domain and experts in the field. The most relevant characteristics of maritime security, identified following an analysis of studies carried out by Institut für Strategie- Politik- Sicherheits- und

[13] Smith-Windsor, B., A. (2013). NATO's Maritime Strategy and the Libya crisis as seen from the sea, accessed from https://www.files.ethz.ch/isn/161498/rp_90.pdf, on the 5th of January 2024.

[14] www.nato.int/nato_static/assets/pdf/pdf_2011_03/20110318_alliance_maritime-strategy_CM_2011_23.pdf, accessed on the 5th of January 2024.

[15] European Union Maritime Security Strategy (EUMSS) nr. 11205/14, Brussels, 24 June 2014.

[16] Maritime Security – Perspectives for a comprehensive approach. Feldt, L., Roell, P. (Dr.), Thiele, R. D. (2013). ISPSW Strategy Series: Focus on Defense and International Security, 222. Accessed from https://www.files.ethz.ch/isn/162756/222_Feldt_Roell_Thiele.pdf, on the 5th of January 2024.

[17] https://www.researchgate.net/publication/270107474_What_is_maritime_security, accessed on the 22nd of December 2023.

[18] https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx, accessed on the 5th of January 2024.

Wirtschaftsberatung ISPSW[19] and which we consider appropriate to any desired maritime security, would be:

- international and national peace and security;
- sovereignty, territorial integrity and political independence;
- security of Sea Lines of Communications;
- security protection from crimes at sea;
- resource security, access to resources at sea and to the seabed;
- environmental protection;
- security of all seafarers and fishermen;
- security of ports and port facilities.

Another aspect that needs clarification is the responsibility for ensuring security in seas and oceans and who holds it. Regarding maritime security responsibility, UNCLOS[20] Convention – actually, a comprehensive set of articles and regulations providing a basis for "good governance at sea" – repeatedly states that all signatory nations become responsible for safeguarding the maritime domain (UN, 1982).

Additionally, as civilian actors view maritime security from an economic and environmental perspective, the responsibility for securing the maritime environment becomes an objective for all stakeholders. Economic agents require stability and certainty to venture investments in the maritime domain; consequently, a safe and secure maritime environment becomes the aspiration of a significant number of actors.

In conclusion, even though there is no universal definition for the term "maritime security," there are approaches that provide clarifications and focus on ideas to consolidate a universally accepted understanding of all aspects of maritime security. The nature of the seas has changed from an open space where freedom was the rule to a common, vast yet fragile domain that requires global management and protection, where regional cooperation is gradually taking place.

2. International and regional cooperation

A prominent trend in the development of maritime security strategies is the emphasis on regional and international cooperation. Many nations acknowledge that maritime threats often transcend their own borders, requiring collaborative efforts to effectively counter them.

In this regard, various forms of regional cooperation and multinational partnerships have emerged to ensure the exchange of information, conduct joint patrols and coordinate responses to maritime incidents. Examples for such cooperation are as follows:

- The MCM (Mine Countermeasures) Black Sea represents the latest formalization of regional cooperation, involving the establishment of a Task Group for countering maritime mines in the Black Sea. This initiative is led by the three Black Sea littoral allies (Romania, Bulgaria and Turkey) and aims to enhance navigation safety by addressing the threats posed by maritime mines[21].
- EU NAVFOR Atalanta is a naval operation of the European Union involving member states and other contributing countries. Its primary objective is to protect commercial vessels against piracy in the Gulf of Aden region.

[19] Lutz Feldt, Dr. Peter Roell, Ralph D. Thiele, Maritime Security – Perspectives for a Comprehensive Approach, April 2023, according to https://www.files.ethz.ch/isn/162756/222_feldt_roell_thiele.pdf, accessed on the 7th of January 2024.

[20] UNCLOS – United Nations Convention on the Law of the Sea.

[21] https://www.mapn.ro/cpresa/18249_ministrul-tilvar-va-semna-la-istanbul-memorandumul-de-intelegere-privind-constituirea-grupului-operativ-pentru-combaterea-minelor-marine-in-marea-neagra---mcm-black-sea, accessed on the 10th of January 2024.

- The International Maritime Security Construct (IMSC) is a coalition composed of several countries, including the United States, the United Kingdom, Australia, Saudi Arabia, the United Arab Emirates and Bahrain. Its objective is to ensure the security of commercial vessels in the Persian Gulf, the Strait of Hormuz and the Gulf of Oman, especially amidst escalating tensions and maritime incidents in the region.
- Combined Task Force 150 (CTF-150) is a multinational force involving countries such as the USA, the United Kingdom, France, Australia and others. It is focused on combating terrorism, countering smuggling and addressing illegal trafficking in the Arabian Sea and the Indian Ocean region.

When referring to NATO, international cooperation is materialized through the Standing NATO Maritime Group (SNMG). This group represents a flexible and integrated force of warships from various NATO member countries, operating throughout NATO's area of responsibility. SNMG aims to ensure maritime presence, respond rapidly to crisis situations and support security in international waters.

The European Union (EU) contributes to maritime security through Operation Irini, focusing on monitoring the enforcement of the embargo imposed on Libya and combating illegal trafficking of weapons and oil in the Mediterranean Sea. This operation involves ongoing cooperation among EU member states to ensure the participation of warships and reconnaissance aircraft, highlighting collective efforts to prevent conflicts and maintain maritime security in the region.

All these relevant examples emphasize the importance of international and regional cooperation for the effective management of maritime threats and the maintenance of security worldwide.

An important aspect of the evolution of the security environment is represented by disruptive technologies. It is observed that technological advancements play a crucial role in the evolution of maritime security strategies. Nations are increasingly using satellite surveillance, unmanned aerial vehicles (UAVs) and advanced sensor networks to increase their maritime domain awareness (MDA). These technologies not only aid in monitoring vast maritime areas but also contribute to optimizing and efficiently utilizing rapid response capabilities in the event of security incidents.

Satellite surveillance provides detailed real-time information, enabling continuous monitoring of naval traffic and suspicious activities at sea. Concurrently, UAVs extend surveillance capabilities in hard-to-reach or challenging areas not easily covered by traditional means. Advanced sensor networks complement this equation by automatically collecting, analysing and reporting data, enhancing a comprehensive understanding of the maritime environment.

These technologies not only transform the way states approach maritime security but also significantly enhance the ability to anticipate and respond to incidents. By integrating them into the maritime security strategy, states become more agile in the face of maritime challenges, optimizing resources and reducing crises response times. Therefore, we believe that disruptive technologies form the foundation of a robust and adaptable maritime security strategy against ever-changing threats.

Last but not least, leadership becomes crucial in regional and international cooperation, considering that Naval Forces are involved and represent important pillars in ensuring and promoting regional and international stability. An effective leader can navigate through the complexity of international relations, facilitating dialogue and promoting mutual understanding between states, contributing to building trust among actors for crisis management, which is essential for strengthening cooperation and achieving common objectives in a globally interconnected context.[22] Therefore, an effective leader within Naval Forces not only guides their team diplomatically, but also prepares them to efficiently respond to specific challenges of maritime security.

3. Examples of maritime security strategies worldwide and future trends

Several countries have developed and implemented maritime security strategies to protect their maritime interests and counter various threats at sea. Below we have analysed and listed some examples of countries known for maritime security strategies:

a) The United States of America:

The United States places a high priority on maritime security due to its global economic interests and strategic position. The US Maritime Strategy emphasizes power projection and cooperation with its allies and partners.

Also, maritime domain awareness (Maritime Domain Awareness), countering emerging threats such as terrorism, cyber-attacks and the proliferation of weapons of mass destruction are priority actions identified by the strategy.

The US Navy plays a central role in implementing the strategy, ensuring the free flow of maritime commerce, protecting maritime resources and responding promptly to potential crises.

b) The United Kingdom of Great Britain and Northern Ireland:

UK's maritime security strategy encompasses defense and security aspects, with an emphasis on protecting sea lines of communication, combating piracy and maintaining a credible naval deterrent.

With the Royal Navy at the fore, the strategy addresses challenges in the Atlantic Ocean, the North Sea and other hot areas of national interest

c) France:

France's maritime strategy involves a combination of national defense and protection of maritime resources. It focuses on protecting French interests in the Mediterranean, the Atlantic and further afield.

The French Navy plays a vital role in executing maritime security operations, including counter-piracy efforts and contributing to international maritime stability.

d) The Netherlands:

The Netherlands emphasizes the importance of international cooperation in its maritime security strategy, especially in the North Sea. It addresses challenges such as maritime terrorism, smuggling and environmental protection.

The Royal Netherlands Navy contributes to regional security through patrols and collaborative efforts with neighbouring countries.

e) China:

China's maritime security strategy is driven by its economic interests and the need to protect sea lines of communication. This involves modernizing its navy and establishing specialized maritime law enforcement entities.

The strategy is particularly evident in the South China Sea, where China has asserted territorial claims and developed naval capabilities to protect its interests.

f) India:

India's maritime security strategy focuses on securing its extensive coastline and exclusive economic zone, and ensuring maritime stability in the Indian Ocean region.

[22] Chiorcea I., Cioranu I. (2021). *Inteligența emoțională în leadershipul militar*, accessed from https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2021%20gmr/2021/1/CHIORCEA%2C%20CIORANU.pdf, on the 7th of February 2024.

The Indian Navy is a key player, conducting regular patrols, contributing to anti-piracy operations, and participating in international maritime exercises to encourage naval cooperation.

g) Japan:

Japan's maritime security strategy focuses on securing sea lanes of communication critical to its economic interests. It focuses on modernizing naval forces and contributing to international efforts to combat piracy.

Japan actively participates in regional security dialogues and exercises, building partnerships to address current maritime challenges.

h) Australia:

Australia's maritime security strategy addresses regional stability, counter-terrorism and the protection of maritime trade routes.

The Royal Australian Navy is a key component, engaged in maritime patrols, contributing to international coalition efforts and collaborating with regional partners.

i) Brazil:

Brazil's maritime security strategy aims to combat illegal activities at sea, including drug trafficking and illegal fishing. Emphasis is placed on the protection of marine resources and the sustainability of the marine environment.

The Brazilian Navy plays a central role in executing strategy, conducting patrols and participating in regional security initiatives.

j) South Africa:

South Africa's maritime security strategy focuses on protecting its maritime interests, securing sea lanes and contributing to regional stability.

The South African Navy conducts patrols and participates in international anti-piracy and maritime security efforts in the Indian and Atlantic Oceans.

*
* *

These examples show the diversity of approaches to maritime security based on each country's unique geographic, economic and geopolitical considerations.

Considering the models of the presented strategies, some framework models could be identified, which combine the same principles of development and implementation, as follows:

1. Strategy based on power projection.
2. Strategy based on contribution to regional security.
3. Strategy based on the defense of interests in the region (deterrence strategy).
4. Strategy based on the protection of maritime resources in the area of responsibility.
5. Strategy based on the defense of interests and the capitalization of resources in the area of responsibility.
6. Strategy based on regional security cooperation.

Considering the identified models, our proposal is the realization of a Maritime Security Strategy based on regional cooperation in the field of security with the defense of interests in the region. The solution aims to involve the shores in strengthening maritime security through the creation or capitalization of existing forums but on common dialogue platforms regarding the application of a common maritime security strategy simultaneously with the promotion of national interests on the sea and river and the promotion of allied and community maritime strategies.

For this reason, we consider that the participants in the development and implementation of this strategy should be the Ministry of National Defense, the Ministry of Internal Affairs, the Ministry of Foreign Affairs, the Ministry of Transport, the Ministry of Economy, the Ministry of Development, agencies and institutions with responsibilities in the maritime field, so that the initiation of the approach must be performed by the Government of Romania, with the support and participation of all the responsible factors in the field of state security, but also by the beneficiary ministries. The argument underlying this proposal is the fact that in such a complex field, as the maritime field, maritime security is impossible to achieve by a single institution, through an independent effort. Moreover, maritime security being a subject of international interest, the active participation of all relevant actors at the regional level will provide active support for common maritime security.

Conclusions

Maritime security has become a priority area in international politics, with increasingly frequent and focused debates around this complex and changing issue. The ongoing development of international events shows that maritime security will remain a central topic in global strategies and policies to ensure world stability and prosperity.

The diversity of strategies adopted by countries around the world highlights their adaptability to the geographical, economic, historical and geopolitical particularities specific to each state. From prioritizing global power projection to models based on regional cooperation or the protection of maritime resources in the area of responsibility, the approaches reflect the complexity of the maritime environment and the need for continuous adaptability.

We are witnessing an increased awareness that maritime threats transcend national borders. Examples such as cooperation within NATO, the European Union, and multinational partnerships highlight the importance of information sharing, joint maritime patrol missions, and coordinated response to effectively manage the inherent challenges of the maritime environment.

We believe that advances in disruptive technologies, such as satellite surveillance, the use of unmanned aerial vehicles, and artificial intelligence, have become key elements in the evolution of maritime security strategies. These technologies not only optimize monitoring and incident response but also transform the way states address the ever-changing challenges of maritime security.

Because the research objectives were met, the results support the fact that the appropriate model of a security strategy in the maritime and fluvial field for Romania is the framework of a maritime security strategy based on regional cooperation and the defense of interests in the region with the assertion of allied will and community.

Taking into account all the aspects presented, Romania could have numerous benefits following the implementation of a maritime security strategy based on regional cooperation. After identifying threats to maritime security and establishing strategic objectives, the next natural step would be to design strategic actions to achieve the objectives. This integrative approach should be initiated at the government level and would involve the active participation of several relevant ministries and institutions, bringing together joint efforts to effectively manage maritime challenges and ensure security and economic prosperity in an ever-changing maritime environment.

BIBLIOGRAPHY:

1. Bueger, Ch. (2015). What is Maritime Security? Marine Policy. Cardiff University. Accessed from http://bueger.info/wp-content/uploads/2014/12/Bueger-2014-What-is-Maritime-Security-final.pdf
2. Feldt, L., Roell, P. (Dr.), Thiele, R. D. (2013). Maritime Security – Perspectives for a comprehensive approach. ISPSW Strategy Series: Focus on Defense and International Security, 222. Accessed from https://www.files.ethz.ch/isn/162756/222_Feldt_Roell_Thiele.pdf
3. NATO (2011) Alliance maritime strategy. Accessed from https://www.nato.int/nato_static/assets/pdf/pdf_2011_03/20110318_alliance_maritime-strategy_CM_2011_23.pdf.
4. United Nations Convention on the Law of the Sea - UNCLOS. Accessed from https://www.un.org/Depts/los/convention_agreements/texts/unclos/unclos_e.pdf.
5. UNCTAD – United Nations Conference on Trade and Development (2010). Review of maritime transport 2010. Accessed on https://unctad.org/en/docs/rmt2010ch1_en.pdf.
6. Chiorcea I., Cioranu I. (2021). Inteligența emoțională în leadershipul militar, accessed from https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2021%20gmr/2021/1/CHIORCEA%2C%20CIORANU.pdf, on the 7th of February 2024.
7. Egli, D. S. (2011). Understanding the role of interagency coordination in national-level maritime security. Accessed on https://search-proquest-com.am.e-formation.ro/central/docview/916422078/849DC44A7CC44724PQ/4?accountid=136549.
8. The European Union Council (2014). EU Maritime Security Strategy. Accessed from http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011205%202014%20INIT.
9. https://www.imo.org/en.
10. https://www.files.ethz.ch/isn/162756/222_feldt_roell_thiele.pdf.
11. https://www.mapn.ro/cpresa/18249_ministrul-tilvar-va-semna-la-istanbul-memorandumul-de-intelegere-privind-constituirea-grupului-operativ-pentru-combaterea-minelor-marine-in-marea-neagra---mcm-black-sea.

1053477-3045-1396-24-37

DEVELOPMENTS OF THE COMMUNITY FISCAL POLICY

Mădălina SCIPANOV, PhD.
PhD., associate professor, National Defence University "Carol I", Bucharest, Romania
E-mail:badea_mad@yahoo.com

***Abstract**: In this article, a comparative analysis of the evolution of the community tax policy is carried out, from the perspective of the national policy as well as at the level of the European Union. Thus, by comparing the two fiscal systems, regarding the fiscal approach at the level of some member states, it will be possible to highlight the particularities of fiscal competitiveness and the impact of taxation on the economy of the European Union. Taxation is a historical result of the social, political, and economic environment at the global, regional, or national level and implicitly individually. It starts from the assumption that the state of development of a state is dependent to a significant extent on the history of its fiscal system, and on the way it is designed and functions. The concern for the study of fiscal policy and the state budget was generated by the importance that a government must give to these monetary policy instruments.*

National taxation represents one of the most dynamic phenomena in the market economy, through which the public authority establishes not only the coordinates of the setting, collection, and control of taxes and fees but also their use more or less as a balancing tool of the management directions of the market. The elaboration of the fiscal policy is a particularly complex act of decision based on the efficiency criterion, that is, the need to establish and obtain the highest possible return on it with the existing resources. The purpose of fiscal policies is to ensure the mobilization of public revenues as high as possible, under the conditions of encouraging economic affairs and investments, simultaneously with the promotion of equity in everyone's contribution to revenues, with the assurance of social protection and the well-being of the individual.

The article, from an epistemological and practical point of view, deals with the issue of taxation and the state budget in Romania, constituting, at the same time, a challenge that supports developments and additions on the part of those interested. Therefore, the novelty of this article starts from the existing realities in the European Union and details a wide spectrum of problems regarding the role of states in the economy, the mechanism of taxation and its improvement under the conditions of macroeconomic stabilization; analyzes the level of taxation in Romania and at the level of the European Union; compares the existing levels of taxation in the European Union, analyzing fiscal competition and the effects on legal entities.

***Keywords**: fiscal policy, community taxation, economic measures, taxation*

Introduction

Within this approach, it is proposed to bring attention to the important role that fiscal policy has within the policies applied by the government to achieve the main macroeconomic objectives, which are usually multiple (for example: a high level of employment; a high rate of economic growth; price stability; balance of external payments), using specific instruments integrated in the fiscal systems applied at a given time.

Fiscality (DEX) it is the system of collecting taxes and fees through the tax office, and the tax office is the state institution that establishes and collects contributions to the state and pursues those who have not paid these contributions. The evolution of taxation is closely related to the evolution of the state and its functions, since as the role of the state increases, the need for financial resources at its disposal has continuously increased.

Taxation is an essential component of international finance and is based on two levers (Mircea Ştefan Minea, 2006):

- fiscal policy – the set of decisions defining and determining the mandatory levies, with influences on the macroeconomic and microeconomic balance;

- fiscal law – the legal rules adopted to establish and maintain all actions regarding the collection, on legal grounds, of the amounts charged as taxes, fees, contributions, etc. by local, central public authorities, and/or international organizations.

In specialized literature, taxation represents the system of establishing state revenues by redistributing national income with the help of taxes and fees, and regulation by legal norms.(G. Marin, A. Puiu, 1993) Although it is considered by taxpayers to be a form of coercion exercised by the state, taxation is a complex, concrete, and juridical field par excellence.

Therefore, taxation is a notion inseparable from the state, being an essential component of the state's general policy that decisively influences economic and social life. It is an exciting topic, generating frequent polemics, especially between authorities and taxpayers.

Thus, the need for ever-increasing financial resources determines the state's tendency to obtain as much revenue as possible from taxes and fees. The fiscal system can be used as a tool for regulating economic life, and for state intervention in the economy to eliminate imbalances from different periods of life. Each state promotes its fiscal policy, establishing the number, type, and amount of taxes and fees borne by taxpayers. They are structured according to different criteria to evaluate and analyze the effects of taxation on the dynamics of the economy. The most used criterion is the one related to legal and administrative characteristics, according to which taxes are divided into direct taxes and indirect taxes.

At the current stage, Romania's economy is not completely stable or independent, so taxes fulfill the role of a fiscal instrument. In the measure of economic stabilization, they must move away from this role and fulfill the function of a stimulating instrument in the regulation of the economy, by supporting some of its branches, but not their maintenance. One of the basic conditions for the consolidation of the market economy is a well-developed fiscal system, in which the fiscal policy has a very important role in the amplification of certain categories of commercial relations, the stimulation and facilitation of the activity of economic agents, the attraction of foreign investments, these being realized by changing the tax rates, establishing a taxation system appropriate to the requirements. All the aspects exposed above and their history show that the fiscal reform and the structure of the state budget in Romania were and continue to be marked by internal and international economic processes.

Therefore, the European Commission invites member states to include in their stability and convergence programs how their fiscal plans will ensure compliance with the 3% of GDP deficit reference value, as well as the plausible and continuous reduction of debt or the maintenance of debt at levels prudent, in the medium term. More specifically, all Member States are invited to set fiscal targets that ensure that the deficit does not exceed 3% of GDP or is reduced below 3% of GDP during the period covered by the stability or convergence program and to take credible measures for the deficit to be kept below 3% of GDP in the case of an unchanged fiscal policy in the medium term.

Member states are also invited to discuss how their reform and investment plans should contribute to fiscal sustainability and sustainable and inclusive growth, especially about the twin goals of green and digital transition and resilience, following the criteria set out in the Commission’s reform guidelines.

The main factors influencing the fiscal policy for the year 2024, which the European Union wants to implement, are taxation in the field of energy, budget expenditures, the reform of the EU's economic governance framework, the deactivation of the general safeguard clause (www.universuljuridic.ro), the review of economic governance, the plans to stability and convergence, efficient use of funds from the Recovery and Resilience Facility and other EU funds (https://www.universuljuridic.ro).

I. Taxation in Romania – developments and effects

It is well known that Romania did not have a very efficient fiscal system, in the history of taxation, corresponding to the requirements of the transition stage to the market economy, carrying out a gradual reform, which did not always generate the expected effects on the economic environment, mainly due to the manifestation of some unfavorable conditions for economic reforms but also the inconsistency between legislative provisions and practical realities.

Fiscal policy is an integral part of the state's economic policy and includes the set of ideas and strategies transposed into legal regulations necessary to determine and implement the forms of withdrawal to the budget of sums of money intended to be spent for public purposes (public revenues). That is why fiscal policy intersects with sectoral policies (industry, trade, agriculture, etc.), with financial-monetary and social policies (Iulian Văcărel, 2003).

The Romanian state procures its revenues from taxes, fees, and contributions, from taxpayers in the process of distributing the gross national product. Taxes, fees, and other revenues, which are collected in the state budget, form a system of budget revenues. The system of budget revenues means all taxes, and fees collected from the state budget, local budgets, and the state social insurance budget.

The budget revenues of the Romanian state form a unitary system, because they express the social-economic relations, regulated by the state in a unitary manner through normative acts, and after their collection, they lose their individuality and are used to carry out state expenses such as national defense, investments, research, budget staff salaries, medical and social services, external contributions (EU budget, IMF), social and cultural activities.

Taxes, fees, and other state budget revenues are of great importance not only as amounts that feed the state budget but also through the influence it exerts on the economic and social activity of the country. That is why the system of budget revenues must be constituted in such a way as to stimulate the development of economic and social activity. Taxes and fees can be instruments for boosting, encouraging or breaking, increasing or reducing the production and consumption of some products, and stimulating or limiting the export of some goods. Tax is an instrument of state intervention in economic and social activity. Taxes represent the second main category of state budget revenues and represent the payment made by natural and legal persons for the services provided to them, directly and immediately by public authorities.

Therefore, taxes are regulated as budget obligations owed by natural persons or legal, representing non-equivalent payment of some services requested by them, to some state institutions, according to the principle of special reward.

In Romania, the fiscal consolidation measures seem more drastic than in the countries of the European Union. We are still in the excessive fiscal deficit procedure, (and by the end of 2024, it will most likely remain in the area of 6%), and the interest rates at which we borrow from external institutions to cover the deficit are above the average of the countries in the European Union.

Although the latest measures to remove some tax breaks and introduce turnover taxation for larger companies with low profitability should bring a narrowing of the tax gap, the effect will be short-lived. Eliminating tax evasion as a viable response from the start, the adaptation of companies to the new restrictive conditions would take place on several levels. If, in the case of the elimination of some tax facilities, the obvious effect would be to increase prices on the distribution chain, in the case of taxing the turnover, the effects will be more extensive.

The fiscal system can be used as a tool for regulating economic life, and for state intervention in the economy to eliminate imbalances from different periods of economic life. Moreover, the relationship between taxation and the level of development of the economy is conditional: a stable, developed economy always reflects an environment conducive to fiscal relaxation (this fact is not always valid at the level of an economy in transition, the reduction of fiscal pressure not having the expected effect on economic development as a result of the tendency of economic operators to divert additional income from the economic circuit).

It can be observed that following the changes in taxation conditions, the year 2024 is a year of increased tax pressure on many taxpayers. The direct or indirect impact of the major changes in the tax legislation from 2023 is already being applied, the expected effect would be to approach the European average of around 40% of GDP. Under these conditions, any taxpayer must understand in advance the implications of the tax changes on him, so that he can properly allocate his attention and resources.

Next, an analysis is made of some important changes that will be applied this year and their implications for taxpayers. The analysis will include two perspectives: the state's need to collect revenues; facilitate economic development and encourage business. The main problem is the fact that the state must achieve a balance between these variables, revenues, and business development. The latter must grow, produce goods, and services, and ensure more and better-paid jobs to be able to pay, thus, higher taxes to the budget.

The revenues that the state forecasts that it will collect in 2024 (308.75 billion lei) are divided into current revenues, amounting to 238.02 billion lei (77.09% of the total), income from capital amounting to 372 .43 million lei (0.12%) and subsidies (in the amount of 59.85 billion lei, respectively 19.38% of total revenues). (Government of Romania, 2024)

Current revenues forecast for the next budget year are higher by 47.53 billion lei (a nominal increase of almost 25%) compared to the revenues collected at the end of 2022 (Government of Romania, 2024), respectively 34.6% higher compared to the current revenues collected at the end of October of the year 2023. (Government of Romania, 2024)

The budgeted current revenues for the year 2024 (Report on the macroeconomic situation for the year 2024) are divided into:

1. Fiscal revenues (taxes and charges) - 200.29 billion lei (nominal increase of 25.5% compared to the end of 2022, 37.7% compared to the end of October 2023, respectively 20.26% compared to the execution preliminary from the end of 2023);

2. Insurance contributions - 15.01 billion lei (an increase of approximately 40%, both compared to the amounts collected until the end of 2022, and compared to the value of these revenues recorded until the end of October 2023. Compared to the preliminary execution from the end of 2023, these revenues increased by 16.63%);

3. Non-tax revenues (including property, interest, sales of goods and services, fines, etc.) - 22.71 billion lei (1.57% increase compared to the preliminary execution from the end of 2023). (Report on the macroeconomic situation for the year 2024)

Income from capital represents the amounts derived from the capitalization of some goods, and the budget for the year 2024 is 26% higher than the receipts recorded until the end of October 2023, respectively 21% lower than the budget year 2022.

One of the structural problems of Romania's fiscal system is the insufficient collection of value-added tax (VAT). This aspect results from the European statistics and constantly warned, the result being losses of tens of billions annually.

Seen in the context in which Romania records year after year low levels of tax revenues (about 27 percent, the penultimate place in the EU after Ireland), losses from VAT collection prevent the state from being able to ensure quality public goods and services.

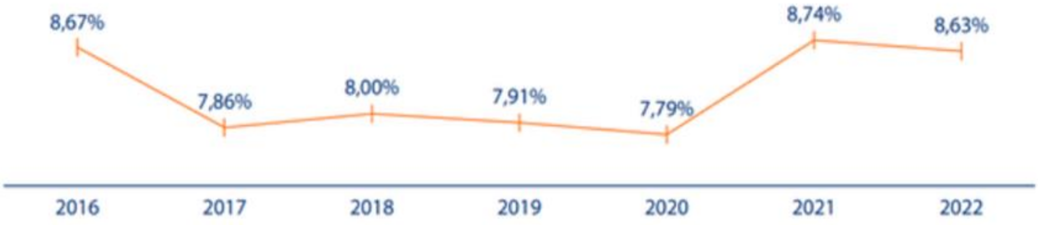


Figure no. 1. Evolution of VAT -annually- in % GDP -2016-2022
Source: https:// https://www.profit.ro

According to specialized reports (https://www.profit.ro), in the graph presenting the evolution of VAT collections from 2016-2022, a downward evolution of collections can be noted in the period 2016-2020 (when the quotas were reduced), followed by an increase in 2021 and 2022. Throughout this period, Romania recorded solid GDP growth, based on the advance of domestic consumption, which would have justified much more serious increases in the share of VAT revenues in GDP.

In 2017, VAT receipts decreased, from 8.67% to 7.86% of GDP (-0.81% GDP, i.e. -10.3%), but the GDP growth is a remarkable one, of 6.9%, growth mainly obtained from the increase in domestic consumption. This decrease can be partly explained by the reduction of the standard VAT rate, from 20% in 2016 to 19% from 1 January 2017, i.e. a decrease of 5.2%.

In 2018, VAT receipts increased slightly, to 8% GDP (+0.14% GDP, i.e. +1.7%), in the context of a solid economic growth of 4.1%, also based on consumption, but in a period when the VAT rate in HoReCa was reduced from 9% to 5%.

In 2019, there was a slight decrease to 7.91% GDP (-0.09% GDP, i.e. -1.13%), although the economy continues to advance by 4%, thanks to consumption. A decrease that can only partly be explained by the extension of the application of the 5% quota to new housing deliveries (under certain conditions) and the introduction of a super-reduced 5% quota for certain foods (especially organic).

Due to the increase in consumption in 2021, an increase in VAT receipts was created to 8.74% of GDP in 2021 (+0.95% of GDP, i.e. +12.2%). The rise in energy prices also contributed to this, as well as deferred VAT receipts for payment in 2020.

In 2022, VAT receipts had a downward trend, dropping to 8.63% of GDP, a rather curious aspect given that energy prices have increased and inflation was at 16%.

From the reports of the Fiscal-Budgetary Strategy for 2024-2026 (Government of Romania, 2024), and the analysis of income tax receipts in Romania, it can be observed that the receipts from salary and income tax totaled 33.30 billion lei, recording an increase of 21.2% (year/year), determined by the increase in receipts from the dividend tax (51.1%) and the tax on pension income (42.0%), At the same time, the income from the salary tax registered an advance of 10.8%, under the evolution of the wage fund in the economy (15.3%), the dynamics of this category of receipts being influenced by the expansion in the agricultural sector and the food industry of the facility granted to employees in construction and the non-taxation of the amount of 200 lei/month for employees who receive the minimum gross salary.

Profit tax receipts, in 2023, totaled 27.49 billion lei, recording an increase of 10.6% (year/year), supported by the advance of profit tax receipts from economic agents (12.8%) and from commercial banks (12.05%) (Government of Romania, 2024). Also, non-tax revenues totaled 37.35 billion lei, recording an advance of 3.9% (year/year), supported by dividend receipts and amounts from the sale of greenhouse gas emissions certificates. On the other hand, there was a decrease in the receipts from royalties - against the background of the downward evolution of energy prices, respectively of payments from the net revenues of the Romanian National Bank. (Government of Romania, 2024)

We now find that the year 2024 brings higher taxes for many companies and individuals and, implicitly, a decrease in income, consumption, and investments. Some of these fiscal changes were anticipated, under the terms of the commitments from the National Recovery and Resilience Plan (PNNR/NRRP), others surprised the business environment.

In conclusion, the tax changes are major and are likely to generate additional financial pressure, as well as a mechanism for taxpayers' resilience, given the complexity of the tax changes. As it emerges from the analysis of the budget situation and the desire to reduce the budget deficit, it is quite likely that the year 2025 will bring more extensive fiscal changes. An expected solution would be progressive income tax, but in my opinion, other fiscal mechanisms could solve the taxation equation in the current fiscal conditions. A proposal aims to connect and facilitate access to community resources for the initiation of an economic mechanism of the future that supports national taxation and the progressive achievement of independence from the community budget.

II. Fiscal policy within the European Union – present and perspectives

The fiscal policy within the European Union consists of two components: direct taxation, which remains the exclusive competence of the member states, and indirect taxation, which influences the free movement of goods and the free provision of services on the single market.(https://european-union.europa.eu) In terms of direct taxation, however, the EU has established harmonized standards on corporate and personal taxation, and member states have taken joint measures to prevent tax evasion and double taxation. In the field of indirect taxation, the EU coordinates and harmonizes legislation on value-added tax (VAT) and excise duties. This avoids the distortion of competition on the internal market as a result of variations in indirect tax rates and systems that would give firms from a certain country an unfair advantage over others.

The European Union does not play a direct role in collecting taxes or setting tax rates. The amount of taxes and fees that each citizen must pay is set by the government of their country. The same is the way of spending the sums collected by the state.

The EU does, however, oversee national tax rules in certain areas, particularly when EU policies targeting businesses and consumers are involved. This is to guarantee that:

- goods, services, and capital can move freely everywhere in the EU (on the single market);
- companies from one country do not benefit from unfair advantages over competitors from other countries;
- taxation is not discriminatory towards consumers, workers, or companies from other EU countries. (https://european-union.europa.eu)

EU decisions in the field of taxation must be unanimously approved by the governments of the member states. This ensures that the interests of each EU country are taken into account. In the case of certain taxes, such as VAT or excise duties on oil, tobacco, and alcohol, the 27 member states must agree to align their rules and minimum quotas, to avoid distorting competition on EU territory. In the case of other taxes, such as profit tax and income tax, the main role of the EU is to guarantee compliance with the principles of non-discrimination and free movement in the single market. There is an increasing need for a coordinated approach at the EU level to help Member States respect these principles and to face common challenges, such as combating tax evasion. The EU does not rule on how the member states decide to spend the revenues obtained from taxation. However, given the growing interdependence of EU economies, countries that spend too much and accumulate too much debt could endanger economic growth in neighboring countries and even undermine the stability of the Eurozone.

To minimize this risk, EU countries try to closely coordinate their policies economic, partly based on the Commission's recommendations. Some of these recommendations refer to national fiscal policies, aiming to make them fairer, more efficient, and more favorable growth. Taxation of businesses and individuals is the responsibility of the Member States. However, according to European rules, they should not put up barriers to mobility in Europe. People who settle in another EU country or companies that invest cross-border may have to pay taxes in at least two countries or face complicated administrative procedures.

Each country in the EU has a standard quota that applies to the supply of most goods and services. This cannot be less than 15%. The EU countries with the highest standard VAT rates are Hungary (27 percent), Croatia, Denmark, and Sweden (all at 25 %). Luxembourg charges the lowest VAT rate on record at 16%, followed by Malta (18%), Cyprus, Germany and Romania (all at 19%). The average standard VAT rate in the European Union is 21%, six percentage points higher than the required minimum standard VAT rate regulated by the EU. In general, excise duties are an economically efficient way to raise tax revenue. To minimize economic distortions, ideally, there is a single standard tariff charged for all final consumption, with as few exemptions as possible. However, EU countries charge lower rates and exempt some goods and services from VAT.

Amounts collected from taxes and social contributions in the European Union increased by €480 billion in 2022 compared to 2021, reaching €6.549 billion, but the share of taxes in EU GDP fell to 41.2% last year, from 41.5%, shows the data published by Eurostat.

Croatia collects the most VAT as a share of GDP among the member states of the European Union but has a standard VAT rate of 25%. The Croatian state collected 13.7% of GDP from VAT, while Denmark and Hungary collected 9.5% of GDP from VAT. Denmark has a standard VAT rate of 25% and Hungary 27%. At the opposite pole is Ireland, which is a statistical anomaly and has a standard VAT rate of 23%, followed by Luxembourg (6% of GDP VAT collection) and Romania (6.2% of GDP). Luxembourg has the lowest standard VAT rate in the European Union – 17%.

The latest annual report on the VAT collection gap produced by the European Commission certifies this fact. According to the Publications Office of the European Union, VAT gap in the EU- Report 2023, one can observe the VAT collection deficit in the European Union. Romania has a VAT collection deficit (calculated as the difference between theoretically collectible VAT and collected VAT) of 36.7%, over 10 percentage points more than the next ranked Malta and at a significant difference from the EU average, of 5.4%. The smallest VAT collection deficits were registered by Finland (1.3%), Estonia (1.8%), and Sweden (2%), and the largest by Romania (35.7%) and Malta (24,1%). EU member states recorded a loss of around €93 billion in value-added tax (VAT) revenue in 2020, down more than €31 billion from the previous year. In recent years, the states in the region have made significant progress in the field of combating tax evasion in the case of VAT, significantly improving their collection yields, as a result of the digitization of national tax administration systems. (European Commission, CASE, Poniatowski, G, et.al.)

Every year, the European Commission monitors the VAT collection deficit because this tax is the most likely to be defrauded and, at the same time, it is among the main resources of the European budget. The deficit represents the losses that state budgets have from VAT due to multiple causes: evasion, fraud, insolvencies, bankruptcy, and administrative errors.

Amounts collected from taxes and social contributions in the European Union increased by €480 billion in 2022 compared to 2021, reaching €6.549 billion, but the share of taxes in EU GDP fell to 41.2% last year, from 41.5%, shows the data published by Eurostat.

According to reports from economedia.ro (https://economedia.ro), an analysis of taxes and social contributions collected in the European Union presents the situation of the countries in the European Union with the highest share of taxes and social contributions in GDP. Thus in 2022, the highest shares of taxes and social contributions as a percentage of GDP will be recorded in France (48.0%), Belgium (45.6%), and Austria (43.6%). Among the member states, Ireland (21.7%), Romania (27.5%), and Malta (29.6%) have the lowest share of taxes in GDP in the European Union. At the opposite pole, the highest share of taxes and social contributions in GDP is registered in France (48%), Belgium (45.6%) and Austria (43.6%). (https://www.profit.ro)

In 2022, compared to 2021, the tax/GDP ratio increased in twelve EU countries, with the largest increases observed in Cyprus (from 34.8% in 2021 to 36.5% in 2022) and Hungary (33, 9% in 2021 and 35.1% in 2022). In Romania, the increase was only 0.3% from 27.2% to 27.5%. The overall tax-to-GDP ratio, i.e. the sum of taxes and net social contributions as a percentage of gross domestic product (GDP), stood at 41.2% in the EU in 2022, down from 2021 (41.5%). In the euro area, tax revenues grew in line with nominal GDP, meaning that the share of taxes in GDP in 2022 remained stable at 41.9%. (https://economedia.ro)

In 2022, according to the previous source (https://economedia.ro), taxes on production and imports accounted for 21.5% of the GDP in Sweden, 19.4% of the GDP in Greece, and 19.2% of the GDP in Croatia. In contrast, these taxes represented only 6.4% of the GDP in Ireland, 10.6% of the GDP in Malta, and 10.7% of the GDP in Romania.

The importance of income and wealth taxes is significant for Denmark, where in 2022 they represented the equivalent of 27.5% of GDP. At the opposite pole, the share of taxes on income and wealth in GDP was only 6.1% in Romania. Capital taxes accounted for 0.3% of EU GDP in 2022, and across member states they range from 0.7% of GDP in Belgium and France.

The conclusion regarding the evolution of taxation within the European Union is that the tax legislation of a country should not allow tax evasion in another member state. Considering the cross-border nature of tax evasion and fraud, permanent communication between the responsible factors in the fiscal-economic field is necessary at the EU level.

Conclusions

The basic condition for the consolidation of the market economy is a well-developed fiscal system, within which the fiscal policy has a very important role in the amplification of certain categories of commercial relations, the stimulation and facilitation of the activity of economic agents, the attraction of foreign investments, achieving - by changing the tax rates - establishing a taxation system appropriate to the requirements.

The reduction of fiscal pressure is another aspect that must involve the provision of an important part or a sufficient part of the revenues at the disposal of economic agents and the population. To achieve this objective, it is necessary to do the following: reduce the overall taxation rate, reduce the number of taxes, change the ratio between direct and indirect taxes (they stimulate saving), decrease the profit tax, and differentiate the rates applied depending on its volume, the branch of activity.

The large number of taxes and some facilities granted by the executive only to certain economic agents, for the payment of budget debts, superimposed on some instability in the legislative field, due to the numerous emergency ordinances of the government with the assumption of responsibility, lead to an unattractive economy for national financiers and international. Government interference is an aspect not found in other economies, whether we are talking about that of the USA or the countries in the E.U. space. This aspect makes a fiscal actor indecisive before deciding to place the capital, to analyze in much more detail the fiscal conditions, the degree of stability of the existing legislation but also an expected legislation, increasing the degree of fiscal risk.

The first conclusion of the present analysis is that Romania remains one of the countries with a complex fiscal system, the consequence being the large number of hours required to pay taxes, fees, and contributions.

Another conclusion is that member states with the highest tax levels tend to show less short-term changes in tax levels than others as if high taxes somehow also introduce elements of rigidity or, in other words, would perpetuate themselves. Many tax cut programs have been announced over the past ten years, but their results have often been modest. This raised the question of whether economic growth could be stimulated by collecting the same amount or a similar amount but in different forms.

Considering the two general conclusions of the analysis, about the partial conclusions, a proposal can be formulated concerning these variables.

Thus, I believe that at the level of the European Union, the governments of the community states must ensure that the tax regimes applied are open and correct and designed in such a way as not to unfairly affect their tax actors, the facilitation of non-Community tax actors, into the detriment of EU policy, or to erode the tax base of primary taxpayers.

At the national level, economic recovery requires extensive programs and strategies, reductions in taxes and fees, or even exemption in certain cases such as job creation, employment stimulation, unemployment reduction, or the use of part of the profit for technology and technical restructuring.

A less highlighted aspect in this analysis is the research component. I believe that encouraging the business environment to invest in research is a starting point for strengthening the fiscal balance of the future. In this case, the state also has a major role in encouraging small and large investors to access funds from European research programs, but also encouraging private, public-private, and public-local initiatives in the development-research field. All these proposals, I believe, will encourage the national fiscal environment, with effects on the national and community fiscal balance.

BIBLIOGRAPHY:

1. DEX, Acadamiei Publishing House, Bucharest, 1996, p. 382
2. Mircea Ștefan Minea, Cosmin Costas – *Fiscalitatea în Europa la începutul mileniului III*, Rosetti Publishing House, Bucharest, 2006, p. 34
3. G. Marin, A. Puiu (coordinators) – *Dicţionar de relaţii economice internaţionale*, Enciclopedica Publishing House, Bucharest, 1993, p. 283
4. www.universuljuridic.ro accesed on 02.02.2024
5. https://www.universuljuridic.ro/orientari-ale-politicii-fiscale-a-statelor-membre-in-2024/ accesed at 02.02.2024
6. Iulian Văcărel (coordinator) – *Finanţe publice,* Didactică şi Pedagogică Publishing House, Bucharest, 2003, p. 109
7. Government of Romania, Fiscal - budgetary strategy for 2024-2026, p.47
8. Government of Romania, according to the general consolidated budget from January 1 - December 31, 2022
9. Report on the macroeconomic situation for the year 2024 and its projection for the years 2025-2027, p.39
10. https://www.profit.ro/taxe-si-consultanta/principalii-indicatori-economici-bugetari- accessed on 29.01.2024
11. Government of Romania, Fiscal - budgetary strategy for 2024-2026, p.49-51
12. https://european-union.europa.eu/priorities-and-actions/actions-topic/taxation_ro accessed on 26.01.2024
13. European Commission, CASE, Poniatowski, G, Bonch-Osmolovskiy, M, Smietanka, A, Sajka, A, *VAT gap in the EU- Report 2023*, Publications Office of the European Union, Luxembourg, 2023
14. https://economedia.ro/romania-penultimul-loc-in-ue-la-veniturile-din-impozite-si-contributii-sociale-in-2022-eurostat.html accessed on 30.01.2024
15. https://www.profit.ro/taxe-si-consultanta/irlanda-si-romania-pe-ultimele-locuri-in-ue-dupa-ponderea-taxelor-in-pib-21366591 accessed on 20.01.2024

16. https://economedia.ro/romania-penultimul-loc-in-ue-la-veniturile-din-impozite-si-contributii-sociale-in-2022-eurostat.html accessed on 01.02.2024
17. Anghelache, Gabriela; Belean, Pavel, Finanțele publice ale României, Ed. Economic& București, 2003
18. Bistriceanu, Gheorghe D., *Sistemul fiscal al Romaniei*, Ed. Universitara, București,2008
19. Brezeanu, Petre; Simion, Ilie; Celea, Sorin, *Fiscalitate Europeana*, Ed. Economick Bucureti, 2005.
20. Vintilă, G. *Taxation: tax methods and techniques*, Economic Publishing House, Bucharest, 2006.
21. https://www.universuljuridic.ro/orientari-ale-politicii-fiscale-a-statelor-membre-in-2024/
22. https://european-union.europa.eu/priorities-and-actions/actions-topic/taxation_ro
23. https://economedia.ro/romania-penultimul-loc-in-ue-la-veniturile-din-impozite-si-contributii-sociale-in-2022-eurostat.html
24. https://www.profit.ro/taxe-si-consultanta/irlanda-si-romania-pe-ultimele-locuri-in-ue-dupa-ponderea-taxelor-in-pib-21366591
25. https://european-union.europa.eu/index_ro;
26. https://eurlex.europa.eu/legalcontent/RO/TXT/PDF/?uri=CELEXI52016DC0148&from=R0)
27. https://ec.europa.eu/taxation_customs/fiscalis-programme_en).
28. https://www.ujmag.ro/economie/fiscalitate/fiscalitate/rasfoire;
29. http://www.cide.ro/caiet_40.pdf ;
30. https://eur-lex.europa.eu/RO/legal-content/summary/the-european-union-s-common-system of-value-added-tax-vat.html;
31. http://europa.eu/eurostat/
32. http://www.strategiimanageriale.ro/images/images_site/articole/article,c.pdf
33. www.mfinante.ro
34. www.bnr.ro
35. www.insse.ro

1053477-3045-1396-24-38

NATO-RUSSIA CONCEPTUAL DIFFERENCES RELATED TO HYBRID THREATS IN THE MARITIME DOMAIN

Adrian Ionuț BĂLAN
Lieutenant Commander, Master's Degree Student, Navy Department, the Command and Staff Faculty, "Carol I" National Defense University, Bucharest, Romania
E-mail: adrianbalan1985@gmail.com

Remus Daniel PINTILII
Lieutenant Commander, Master's Degree Student, Navy Department, the Command and Staff Faculty, "Carol I" National Defense University, Bucharest, Romania
E-mail: pintiliidaniel@yahoo.com

Abstract: *The purpose of this article is to analyze the conceptual and strategic differences between NATO and Russia regarding the management of hybrid threats in the maritime domain. It emphasizes how the two entities perceive and approach maritime security, highlighting the contrast between NATO's approach, which is centered on collective defense, democratic principles, and international cooperation, and Russia's strategy, focused on the use of force and hybrid tactics to extend its influence and challenge the existing international order. The article underscores the importance of dialogue and international cooperation in effectively addressing security challenges in an increasingly globalized and interconnected maritime environment. It argues that confronting hybrid threats requires a multidimensional and flexible perspective, capable of integrating various capabilities and promoting innovative solutions to ensure maritime security and prevent the escalation of tensions. Through this comparative analysis, the article contributes to the understanding of the complexities and dynamics of current maritime security, emphasizing the need for a proactive and adaptable approach to navigate the landscape of international security marked by hybrid threats and increasing geopolitical tensions.*

Keywords*: threats, hybrid, maritime, NATO, Russia*

Introduction

Our goal in writing this paper was to explore the intricacies of maritime security, beginning with a thorough examination of the maritime domain's strategic significance for both domestic and global security. We draw attention to the crucial role that seas and oceans play in international trade and the sustainable management of natural resources, underscoring the extent to which maritime stability and security are critical to the global economy. This section serves as an introduction to the article's main idea and lays the groundwork for future topics.

Hybrid threats, characterized by a complex combination of military and non-military tactics, pose a significant challenge to maritime security. We examine how these threats, through their elusive and multifaceted nature, complicate detection and counteraction, highlighting the need for innovative and multidimensional strategies for effective defense in this new operational theater.

We next turn to a comparative study of NATO and Russian maritime military doctrines, highlighting the disparities in each organization's approaches to maritime security issues and hybrid threats. This part not only shows how major powers' foreign policies and core principles differ from one another but also how these variations affect international stability and global marine security. The study emphasizes the geopolitical complexity of maritime security and the requirement for a thorough knowledge of the dynamics at play by contrasting the strategies of Russia and NATO.

Finally, in light of hybrid threats, we hope to offer a thorough and nuanced analysis of the strategic significance of maritime security. The necessity of a proactive and flexible strategy that can react to the ever-evolving dynamics of the global security environment is emphasized. Our paper seeks to further scholarly and policy discourse by offering a strong foundation for the creation of successful defense plans and global marine cooperation. By using this strategy, we hope to promote international efforts to uphold marine security worldwide and foster a greater awareness of the issues facing the industry today.

Geopolitical context

The maritime domain is essential for preserving both domestic and international security because of its vital location concerning commerce routes, natural resources, and the strategic importance of territorial waters. Since the majority of international trade in today's globalized world occurs over water, maritime trade routes are vital to the world economy. The security of these channels is essential to the uninterrupted flow of products, including food and energy supplies, underscoring the extent to which states depend on a stable and secure sea domain. (Tims 2022)

Seas and oceans are home to a wealth of natural resources, including fishing grounds, different minerals, and hydrocarbon deposits like oil and natural gas, all of which are valuable beyond their commercial application. The preservation and sustainable management of these resources is a top issue for many nations since they are vital to their economy but may also lead to tensions and conflicts.

Territorial seas and exclusive economic zones are strategically significant from a military perspective as well, providing tactical and operational benefits. A state's ability to defend vital infrastructure, such as underground communication cables and gas and oil pipelines, and to monitor and regulate marine operations, including the naval movements of possible adversaries, is ensured by its authority over specific maritime areas.

A favorable environment has been created for the deployment of novel tactics that have the potential to impact not only maritime security but also the world economy, as a result of the escalation of geopolitical tensions and competition for dominance in some maritime regions. Using hybrid threats is one way a state or regional actor might increase its power and sway opinions without starting a confrontation.

In order to gain a strategic advantage, destabilize societies, and jeopardize the national security of the targeted countries, state and non-state actors simultaneously engage in a complex combination of military and non-military acts that constitute these types of threats. Cyberattacks, propaganda and misinformation campaigns, the deployment of special troops, the encouragement of separatist or insurgent organizations, and the taking advantage of political and economic weaknesses are a few examples of these tactics. Hybrid threats complicate the process of attribution and defeating these assaults since they are designed to be below the threshold of conventional warfare and frequently below the level of detection or an effective reaction by the target. (NATO, Understanding hybrid threats 2023)

After emphasizing the importance of the maritime domain and defining hybrid threats, we will compare and contrast NATO and Russia's maritime military doctrines, with a focus on the use of and reaction to these types of threats.

NATO's perspective

A dynamic security environment confronts the North Atlantic Treaty Organization, including a daring Russia that is keen to reshape the global order to its advantage. NATO, its member states, and its allies face a variety of challenges as a result of this altered defense picture. These challenges are especially apparent in the maritime domains surrounding and inside Europe. An Alliance that has concentrated on expeditionary operations and crisis management with a terrestrial concentration for the past ten years faces substantial challenges due to the evolving maritime security environment. (Morcos 2020)

The emergence of hybrid threats has been a prominent topic in the European security paradigm in the wake of recent conflicts. While some may view this as a novel field of study, this idea is fundamentally historical, dating back to the first days of hostilities and warfare. But it has had a tremendous metamorphosis, spurred on by the changing dynamics of the security environment as well as the introduction of innovative instruments, theories, and technological advancements. (E.U. 2022) These developments make it possible to exploit weaknesses in previously unheard-of ways across several domains. Advancements in hybrid threats toolkit expand their capacity for manipulation and infiltration with the goal of accomplishing wide-ranging strategic goals. These goals include weakening public confidence in the democratic system, widening national and international divisions, undermining the cornerstones of democratic societies, gaining the power to dominate geopolitics by adversely affecting others, and impairing the ability of political leaders to make decisions. As a result, it is not unexpected that decision-makers now view hybrid threats as a serious and urgent concern to NATO and its member states, one that requires careful consideration. (Aho A. 2023).

In 2010, the first document referring to hybrid threats, "*Bi-SC Input for a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats*", was drafted by specialists from SHAPE and experts from member states. (NATO, Bi-SC Input to a New NATO Capstone Concept for The Military Contribution to Countering Hybrid Threats 2010)

The operational backdrop discussed in the document has drastically changed as a result of globalization, improved accessibility to resources worldwide, and developments in contemporary communication. Furthermore, regional instability contributes to this change and poses a serious concern in the form of hybrid threats. It also explores a number of modern facets of the hybrid danger. The global interconnectedness of today's globe attracts opponents who may work together and spread misinformation via instantaneous information networks. They can also take advantage of a variety of laws and norms, such as international laws, employment policies, and national limitations, by employing a variety of strategies. This latter point is more important because it clarifies the main components of the hybrid threat and fits in with its definition. According to the document, terrorism, espionage, cyberattacks, conventional lethal and non-lethal weapons, chemical, biological, radiological, and nuclear materials, and criminal activities can all combine to form a hybrid threat. These elements are further supported by an informational system that is intended to spread both false and accurate information through commercial organizations. (NATO, Bi-SC Input to a New NATO Capstone Concept for The Military Contribution to Countering Hybrid Threats 2010)

The comprehension of NATO's strategies and policy for maritime security is crucial in determining how the Alliance approaches challenges in the maritime domain. The NATO Maritime Strategy, updated in 2011, establishes the framework for the Alliance's maritime actions and emphasizes four main roles of its maritime forces: deterrence and collective defense, crisis management, cooperative security, and maritime security. These are linked together and show a comprehensive strategy for maritime security that includes preventive measures, direct military actions, collaboration with partner nations, and engagement in international organizations. (NATO, Alliance Maritime Strategy 2011)

In order to improve efficiency and effectiveness, these missions require NATO's maritime capabilities and organization to be continuously evolved. Since no military force can accomplish security and defense goals on its own, NATO must be more accommodating to all segments of the maritime community. This includes, as the Action Plan for an Integrated Approach specifies, international and regional organizations, non-governmental organizations, and maritime law enforcement agencies, as well as partner and non-partner states as needed. NATO troops must be extremely flexible, adaptable, and versatile in order to meet these demands. They also need to be well-equipped and ready to move quickly and operate from strategic distances, all the while maintaining complete interoperability with their relevant military and civilian counterparts. All NATO operations adhere to international law, including relevant treaties and customary law, as well as any applicable resolutions of the United Nations Security Council. (NATO, Alliance Maritime Strategy 2011)

Another important document referring to hybrid threats is the 2019 annual report of the NATO Secretary-General, which specified the following:

a) In order to gain political and strategic advantages, hostile powers employ non-combative tactics like disinformation, cyberattacks, deception, and sabotage. These tactics blur the lines between peace and war through hybrid activities or in the grey area, intending to destabilize the targeted countries. NATO prioritizes countering these hybrid threats, with members ready to defend one another as part of collective defense, even though the targeted nation bears primary responsibility for reacting to hybrid strikes. (NATO, The Secretary General's Annual Report 2019)

b) NATO works with partners and international organizations to enhance cyber defense, improve intelligence services and early warning systems, and fortify resilience in order to combat hybrid threats. A NATO-level crisis management exercise that tested the Allies' capacity to respond to threats in the political, economic, and military spheres as well as a major meeting at NATO headquarters where Allies exchanged experiences and deliberated methods to enhance support marked the intensification of activities in 2019. (NATO, The Secretary General's Annual Report 2019)

c) Furthermore, the European Centre of Excellence for Countering Hybrid Threats in Helsinki, Finland, has been a vital forum for discussions between NATO and the EU since its establishment in September 2017 and has produced important work on education, training, exercises, and strengthening resilience against hybrid threats. As a result, cooperation with the EU has been strengthened. (NATO, The Secretary General's Annual Report 2019)

Based on an analysis of all alliance papers pertaining to these dangers, NATO has adopted a strong defensive posture in the maritime domain to counter hybrid threats, which reflects the dynamic and intricate nature of contemporary global security problems. The main strategic pillars of this policy are boosting international and regional collaboration, enhancing situational awareness, and creating quick and efficient response capabilities. (Rühle 2021)

The first pillar, improving situational awareness, involves the use of advanced surveillance and reconnaissance technologies to monitor suspicious activities in critical maritime areas. This makes it possible for NATO to promptly recognize and evaluate possible hybrid threats, including disinformation campaigns meant to undermine maritime security, cyberattacks against vital maritime infrastructure, and unconventional naval operations.

The second pillar, strengthening international and regional cooperation, recognizes that hybrid threats do not respect the alliance's borders and, therefore, require a coordinated response. NATO maintains close connections with allies across the globe, including the European Union, littoral states, and regional organizations, in order to coordinate training exercises, standardize reaction procedures, and share intelligence. The alliance's capacity to react to hybrid incidents in a coordinated and efficient manner is improved by this collaboration.

And finally, NATO's maritime defense strategy depends on building quick and efficient response capabilities. This entails arming naval forces with the means to conduct defense and deterrent operations against possible aggressors in addition to fortifying the cyber protection of communication networks and maritime infrastructure. In order to resist hybrid warfare efforts, it also entails creating strategies, tactics, and protocols. Examples of these include using special forces and conducting covert operations to neutralize threats before they can have a major effect.

In summary, NATO's defensive strategy in the maritime domain against hybrid threats is a multifaceted and intricate process that necessitates ongoing innovation, international collaboration, and dedication to maintaining maritime security despite a variety of obstacles. In an ever-changing security landscape, NATO hopes to preserve its strategic edge by taking a proactive and flexible strategy.

The russian perspective

By 2023, the world security system and NATO's place in it had been characterized by a number of different threats, with no one organization being named as the North Atlantic Alliance's main enemy. In order to represent the complexity of the post-Cold War security environment, this dynamic of international security was defined by dealing with a wide variety of hazards, from cyberattacks and international terrorism to regional crises and hybrid threats. But after the 2023 NATO Summit in Vilnius, which signalled a shift in the Alliance's approach and language, things drastically shifted.

At this summit, NATO's stance towards Russia was clarified, unequivocally establishing it as the primary threat to the security of the alliance. Numerous causes, such as Russia's aggressive actions in the Ukrainian region, its military operations in other sovereign states, and its disinformation campaigns and cyberattacks targeted at NATO member nations, all had a role in this. NATO's security strategy has to be adjusted as a result of these actions, which exposed not only a breach of international law principles but also a flagrant disregard for Euro-Atlantic security and values. (Sean Monaghan 2023)

By explicitly recognizing Russia as the principal adversary, NATO reaffirmed its commitment to strengthen its collective defense and to increase investments in military capabilities, including in the cyber and hybrid warfare domains, to ensure credible deterrence and robust defense against any form of aggression. Additionally, this summit emphasized the need for enhanced internal cohesion and closer collaboration among member states, as well as with other international organizations, to effectively face the challenges posed by Russia's behavior.

Analyzing Russia's strategies and doctrine in-depth is crucial for reframing its position, particularly concerning the employment of hybrid threats in the maritime sphere. Understanding the tactics Russia uses to enforce its geopolitical goals and expand its influence, while also seriously undermining NATO's collective security and global stability, makes this research especially crucial.

Theoretical works by Russian generals like Gerasimov and Primakov, as well as previous influences from Soviet General Ogarkov, form the conceptual foundations of hybrid warfare and hybrid threats in Russia. The idea is to accomplish strategic goals by combining military and non-military tactics, such as information manipulation, psychological operations, non-governmental organization utilization, and cultural and economic impact initiatives. The use of cutting-edge technologies like directed energy weapons and robotics in combat operations is another aspect of hybrid warfare, which represents a significant change in the parameters and character of contemporary warfare. This strategy, which goes beyond the conventional paradigm of massive armies, indicates an adaptation to the belief that total political authority and control over certain resources or areas are necessary for victory. (Valori 2020)

Although on a much smaller scale than the annexation of Crimea in 2014, a good example of Russia's successful use of hybrid tactics was the takeover of Kabul following the withdrawal of US troops from Afghanistan. Russia has used a variety of power tools to overcome the Afghan security forces and political system. These tools, along with covert actions of seemingly irresponsible individuals and insignificant fighters, as well as a joint military operation between these individuals, proved to be among the most successful operations conducted by Russian special forces. (Valentin MAXIM 2021) Following the lessons learned from this successful operation, this kind of approach has been extended to other areas, such as, for example, the maritime one.

Russia's approach to countering hybrid threats in the marine domain is centered on an integrated strategy that integrates military and non-military elements. This includes using socio-economic operations and maritime law to further Russian national objectives. The Russian Maritime Doctrine of 2022 places a strong emphasis on the development of port facilities, commercial and civilian fleets, and the capacity for mobilization in the maritime domain. It also highlights the significance of maritime security. It gives special attention to building offshore pipeline infrastructure for the transportation of hydrocarbons, securing Russia's economic independence and food security, and raising the number of ships waving the Russian flag. The doctrine also emphasizes the necessity of addressing the Kerch Strait's international legal regulation and the significance of building the Northern Sea Route as a year-round, safe commercial route. (Chiriac 2022)

Besides these characteristics, Russian political and strategic thought exhibit a vertical power structure that is reflected in the marine ideology. Under this system, maritime or energy resources are viewed first as instruments of power and then as sources of economic or civilian resources. (Chiriac 2022) Furthermore, attention is given to adjusting to regional peculiarities, including those of the Black Sea and the Arctic, acknowledging the necessity of distinct regional strategies to stay current and successful in the face of threats to international security. (Chiriac 2022)

As General Valery Gerasimov has pointed out, Russia's hybrid approach avoids direct confrontations with superpowers like the US in favor of influencing public opinion and controlling the informational landscape in order to further Russia's political goals. This strategy relies on the coordinated application of political, economic, informational, and humanitarian measures in addition to the possibility of public protest. It highlights the growing relevance of non-military tactics in accomplishing political and strategic objectives. In his argument that hybrid tactics—particularly non-military measures—should be employed four times more frequently than traditional military capabilities, Gerasimov highlights Russia's determination to use all available means of national power to subtly influence the operational environment. (Major Valerie McGuire 2018)

Russian military writers like Georgy Samoilovich Isserson and Evgeny Messner have made a substantial contribution to the definition and development of hybrid warfare in Russia. Messner discussed a new kind of warfare that emphasized psychological dominance and the goal of creating mistrust and terror in the opponent in order to destroy the West without resorting to direct military conflict. His theories were later taught in Russian military academies, where they were interpreted as part of the country's hybrid warfare strategy, which aims to undermine and divide the opponent from within by combining military operations with non-military forms of pressure. (Nicolescu 2017)

Different methods and interpretations of this type of conflict are highlighted by comparing the analysis of hybrid conflict from the perspectives of Western and Russian scholars. According to Russian analysts, a conflict only crosses the line into hybrid warfare when the aggressor state seeks overtly to alter the target state's strategic orientation and "worldview". This approach is a reflection of a strategic viewpoint that places more emphasis on long-term social and policy changes in the targeted governments than it does on short-term military gains or territory acquisitions. (Clark 2020)

Like its Western counterparts, the Russian military describes hybrid means using a number of terminology that are frequently interpreted in an ambiguous manner. Actions that are beyond the confines of conventional kinetic military operations are referred to by terms like "hybrid conflict," "hybrid means," "asymmetric operations," "information warfare," "non-military combat," and "non-traditional warfare". The awareness of a wide range of techniques and methods that can be applied to accomplish strategic objectives in an increasingly intricate and linked security environment is reflected in this terminological diversity. (Clark 2020)

Key elements of Russia's hybrid warfare strategy include military presence and force displays, with the goal of expanding its influence both regionally and globally, particularly in the marine sector. (Rácz 2017) This strategy is centered on the visible and calculated deployment of naval troops in key geopolitical locations, like the Mediterranean, the Baltic Sea, and the Black Sea, which are vital for both the projection of global military power and European trade and security.

Since annexing Crimea in 2014, Russia has greatly increased its naval presence in the Black Sea. Russia needs this region strategically because it gives it access to warm waters and allows it to project influence into the Middle East, the Balkans, and beyond. Russia's military prowess is showcased by the deployment of naval manoeuvres and military drills in the Black Sea, which also helps to ward off NATO intervention and other foreign forces seen to be in its sphere of influence. (Gressel 2021)

Russia uses force in the Baltic Sea to reaffirm its interests in opposition to NATO expansion and US military presence in the area. Warship deployments and naval drills aim to expose weaknesses in Northern Europe's security framework, raise tensions, and test the defensive capacities of the Baltic nations and their allies. (Chang 2021)

Due in part to its engagement in the Syrian crisis and the construction of a permanent presence at the naval station in Tartus, Syria, Russia's naval presence in the Mediterranean, particularly in the eastern Mediterranean, has expanded recently. Russia now has a tactical advantage that it may use to project military might not only in the Middle East but also in North Africa and along NATO's southern flank. Russia's ability to send forces outside of its boundaries and to step in during regional crises is demonstrated through naval operations in the Mediterranean, which helps to solidify Russia's standing as a significant player in the world.

Russia aims to protect its interests domestically, increase its clout in neighboring areas, and prove that it is capable of upending the US-led international system. These goals are achieved through military drills and force displays. Additionally, this strategy seeks to reveal the vulnerabilities of allies and enemies and negotiate from a position of strength in global affairs. (Michael Kofman 2015)

The Russian Foreign Minister, Sergey Lavrov, stated during a session of the Council on Foreign and Defense Policy that "The West has declared a total hybrid war on us and it's hard to predict how long all this will last, but it's clear that everyone, without exception, will feel the consequences". (Lavrov 2022) In the context of these statements and through the foreign policy that Russia promotes, it is evident that under the dome of defensive strategy, in fact, predominantly offensive actions are hidden.

Thus, NATO concentrates on collective defense and upholding an order founded on international law, whereas Russia seems to embrace a hybrid warfare strategy with offensive aspects intended to increase its influence and destroy international cohesion. This basic difference in strategy represents the ideals and guiding principles that these companies adhere to on the international scene in addition to the disparities in foreign policies.

The complicated nature of maritime security in the current setting is reflected in the dynamic between Russia and NATO. Maritime security is still a sensitive and crucial topic as all parties seek their own interests and strategic goals.

Conclusions

The conceptual and strategic distinctions between NATO and Russia with regard to hybrid threats in the maritime domain are analyzed, and the results provide a complex picture of goals, strategies, and moral arguments that have a significant impact on the dynamics of international security. NATO is a transatlantic alliance founded on democratic values and collective defense. It emphasizes the rule of law, transparency, and international cooperation in its efforts to ensure the security of its members through political and military methods. However, Russia is taking a more assertive stance to regain its influence in the area and worldwide. This is often done by going it alone or by using force, all of which is justified by the country's need to protect its security and interests.

The divergent goals are a reflection of different perspectives on the global order: Russia seems to be seeking a rebalancing of power, giving preference to its own zone of influence, while NATO advocates a strategy based on international laws and conventions. In terms of approaches, Russia has demonstrated a readiness to use force or hybrid tactics in order to accomplish its goals, whereas NATO advocates discussion, diplomacy, and, as a last option, military intervention based on the agreement of its members.

These distinctions have important worldwide ramifications that raise tensions, spur strategic rivalry, and occasionally result in direct or indirect hostilities. This dynamic makes it more difficult to uphold world peace and stability, which emphasizes the necessity of constant communication, understanding, and the pursuit of amicable resolutions to international conflicts. The international community needs to maintain vigilance and foster a balance between upholding democratic values and the need to prevent conflict from getting worse in order to effectively navigate this complicated terrain.

It is evident from the material that has been made available thus far that NATO must create a Black Sea policy in order to thwart and counteract any unfavorable actions or policies by Russia. A defensive stance that places unaffordable costs on any initial Russian entry through diplomatic, military, economic, and strategic channels could be part of this plan. A thorough discussion of potential war scenarios and the need for such a plan indicates that NATO needs to be ready to react swiftly and decisively to any kind of aggression or disturbance in the area.

Concluding from the above and from the statement that war begins long before the first bullet is fired it is clearer than ever, that Romania needs a maritime defense strategy that includes responses to all types of new threats and through which to protect and promote its interests in the Black Sea.

BIBLIOGRAPHY:

1. Aho A., Alonso Villota M., Giannopoulos G., Jungwirth R., Lebrun M., Savolainen J., Smith H., Willkomm E. *Hybrid CoE.* April 20, 2023. https://www.hybridcoe.fi/publications/hybrid-threats-a-comprehensive-resilience-ecosystem/ (accessed January 25, 2024).
2. Chang, Felix K. *FOREIGN POLICY RESEARCH INSTITUTE.* December 14, 2021. https://www.fpri.org/article/2021/12/crowded-pond-nato-and-russian-maritime-power-in-the-baltic-sea/ (accessed January 25, 2024).
3. Chiriac, Olga R. *CIMSEC.* November 28, 2022. https://cimsec.org/the-2022-maritime-doctrine-of-the-russian-federation-mobilization-maritime-law-and-socio-economic-warfare/ (accessed January 25, 2024).
4. Clark, Mason. "RUSSIAN HYBRID WARFARE." *MILITARY LEARNING AND THE FUTURE OF WAR SERIES*, September 2020: 18-20.
5. Gorenburg, Dmitry. *EUROPEAN CENTER FOR SECURITY STUDIES.* July 2019. https://www.marshallcenter.org/en/publications/security-insights/russias-naval-strategy-mediterranean-0 (accessed February 09, 2024).
6. Gressel, Gustav. *EUROPEAN COUNCIL ON FOREIGN RELATIONS.* September 21, 2021. https://ecfr.eu/publication/waves-of-ambition-russias-military-build-up-in-crimea-and-the-black-sea/ (accessed February 09, 2024).
7. Lavrov, Sergey. *The Ministry of Foreign Affairs of the Russian Federation.* May 14, 2022. https://mid.ru/en/foreign_policy/news/1813377/ (accessed February 07, 2024).
8. Major Valerie McGuire, U.S. Marine Corps. *U.S. Naval Institute.* August 2018. https://www.usni.org/magazines/proceedings/2018/august/hybrid-warfare-helps-russia-level-playing-field (accessed January 23, 2024).
9. Michael Kofman, Matthew Rojansky. "A Closer look at Russia’s “Hybrid War”." *KENNAN CABLE*, April 2015: 1-8.
10. Morcos, Pierre. *CENTER FOR STRATEGIC & INTERNATIONAL STUDIES.* December 03, 2020. https://www.csis.org/analysis/nato-2030-charting-new-path-transatlantic-alliance (accessed February 07, 2024).
11. NATO. "Alliance Maritime Strategy." *www.nato.int.* June 17, 2011. https://www.nato.int/cps/en/natohq/official_texts_75615.htm (accessed January 09, 2024).
12. NATO. "Bi-SC Input to a New NATO Capstone Concept for The Military Contribution to Countering Hybrid Threats." *www.act.nato.int.* 2010. http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf (accessed February 09, 2024).
13. NATO. *The Secretary General’s Annual Report.* Report, NATO, 2019.
14. NATO. *Understanding hybrid threats.* August 18, 2023. https://www.nato.int/cps/en/natohq/topics_156338.htm (accessed January 8, 2024).
15. Nicolescu, Florina Mihaela. *INTELLIGENCE in your service.* 18 December 2017. https://intelligence.sri.ro/razboiul-hibrid-perspectiva-conceptuala-rusa/ (accesat January 26, 2024).
16. Rácz, András. *Russia’s Hybrid War in Ukraine.* FIIA report 43, The Finnish Institute of International Affairs, 2017.
17. Rühle, Michael. *CEPA.* March 22, 2021. https://cepa.org/article/natos-unified-response-to-hybrid-threats/ (accessed January 19, 2024).
18. Sean Monaghan, Sissy Martinez, Otto Svendsen, Carlota García Encina, and Mathieu Droin. *CENTER FOR STRATEGIC & INTERNATIONAL STUDIES.* July 14, 2023. https://www.csis.org/analysis/what-happened-natos-vilnius-summit (accessed February 12, 2024).
19. STEVEN HORRELL, MAGNUS NORDENMAN, WALTER B. SLOCOMBE. "Updating NATO's Maritime Strategy." *Atlantic Council*, 2016.

20. Tims, Catherine. *EHSIsights.* August 7, 2022. https://www.ehsinsight.com/ blog/maritime-security (accessed January 9, 2024).
21. Union, The Diplomatic Service of the European. *EU.* March 03, 2022. https://www.eeas.europa.eu/eeas/countering-hybrid-threats_en (accessed February 07, 2024).
22. Valentin MAXIM, Lucian Valeriu SCIPANOV. „CONSIDERATIONS ON RUSSIAN DOCTRINE AND A NEW MODEL OF WARFARE IN THE BLACK SEA REGION.” *Strategic Impact 78*, January 2021: 63-73.
23. Valori, Giancarlo Elia. *ModernDiplomacy.* June 26, 2020. https://moderndiplomacy.eu/ 2020/06/26/the-theory-of-hybrid-warfare-as-developed-by-generals-gerasimov-and-primakov/ (accessed January 20, 2024).
24. Zaharia, Cristina. *G4media.* February 21, 2022. https://www.g4media.ro/ (accessed February 08, 2024).

SECTION 4

HYBRID WARFARE AND CRITICAL INFRASTRUCTURES PROTECTION

1053477-3045-1396-24-39

SEMI-PERMANENT FACILITIES – CHALLENGES AND OPPORTUNITIES FOR INCREASING THE ADAPTABILITY AND EFFICIENCY OF ROMANIAN MILITARY INFRASTRUCTURE

Adina SEGAL, PhD. candidate
Captain, architect, PhD. student in architecture, Domain and Infrastructure Directorate,
Romanian Ministry of National Defense, Bucharest, Romania
E-mail: segaladina@gmail.com

Abstract: *In the rapidly evolving landscape of today's world, where change is the only constant, the ability to adapt swiftly and efficiently to new circumstances has become essential. Even more so in the realm of military infrastructure where the implementation of a real estate investment is not only a costly and time-consuming endeavour but also filled with complexity due to the necessity to comply with both national legislative frameworks and departmental regulations.*

This article explores the regulations and technical solutions for semi-permanent constructions, a category of structures that hold the potential to provide the armed forces with the necessary facilities promptly and under economically efficient conditions. Beyond merely outlining the current regulations for military infrastructure, the aim is to offer a forward-looking perspective by concluding with a series of considerations on how to better regulate semi-permanent facilities and increase efficiency in the provision of military facilities.

Keywords: *military infrastructure, military constructions, semi-permanent facilities, construction legislation, military regulations.*

Much of the existing Romanian military infrastructure in use today was constructed in the last century, based on standardized projects and regulatory norms for military infrastructure that have since become outdated. The efforts to harmonize regulations with international counterparts have resulted in some inconsistencies with existing national construction laws. This paper conducts an analysis of the regulations governing the implementation of military real estate investments and, by examining the legal and operational constraints, it offers insights into how these structures can be developed more efficiently and effectively. The article concludes with a series of considerations aiming to bring Romania's military infrastructure regulations in line with both national legislative frameworks and current international practices.

I. Romanian Military Infrastructure: Evolution and Standardization

Romania's military infrastructure has experienced significant transformations over the last century, evolving through three distinct development phases, each phase has been closely tied to the historical context and the evolution of the permanent army.

Initially, the military adapted existing structures like inns for immediate operational needs, reflecting the improvised nature of early facilities. This approach quickly shifted to developing specialized military constructions for more complex functional spaces. Post the Union of the Romanian Principalities, the military infrastructure expanded significantly, transitioning to a pavilion system in barracks design. This era marked the beginning of innovation and standardization in military construction, highlighted by the adoption of the *Regulamentul Casarmelor* in 1863, which established norms for space and equipment in barracks. (Herjeu, 1902)

During World War I and II, the focus on barracks intensified, leading to significant investments in permanent constructions. The post-war period saw further changes with the construction of pavilions to expand existing barracks and the adoption of a simplified architectural style. The 1960s focused on modernizing existing infrastructure, with a focus on construction efficiency. Military construction underwent a standardization process, introducing preliminary design phases and generalizing the use of standard projects, coupled with a reorganization of the regulations for infrastructure. In 1975, the *Normele tehnice de cazare* were introduced, the norm which remained active until the next reform series. (Târzioru, 1995)

Post-1989, political, economic, and military transformations necessitated a restructuring and reorganization of the army. Romania's NATO and EU accession led to a re-evaluation of the existing infrastructure and the transfer of numerous military bases to civilian use. The infrastructure regulations introduced in 2008 marked a shift in managing military infrastructure, aiming to align with contemporary international norms. This approach brought in innovative ideas regarding different types of military facilities, ensuring they meet the latest global standards.

This evolution of Romania's military infrastructure from Western models to the Soviet and back to Western standards underscores the need for a dynamic and updated approach to military construction, crucial to meet the evolving demands of national defense.

II. Military Facility Types: an Examination of Semi-Permanent Buildings

Over the last 30 years, there has been a shift from a strictly national territorial defense approach to a strategy that involves the military contributing to collective security (Otu 2009, p. 332). The primary objective of the military reform is to develop a flexible force structure, adequately equipped, deployable, and interoperable both domestically and within allied contexts (Ministerul Apărării Naționale, 2021). The first phase of the transformation process, focusing on completing the basic restructuring, also involved the formulation of regulatory frameworks in the military construction sector (Ministerul Apărării Naționale, 2007).

The 2008 *Regulamentului proprietății imobiliare în Ministerul Apărării Naționale*[23] introduced a new approach aimed at promoting modern building technologies. These technologies support the flexibility required for rapid response and adaptability in military infrastructure and provide solutions for deployed forces. This classification system categorizes the facilities into four distinct types – initial, temporary, semi-permanent, and permanent – based on their intended usage duration and the complexity of their construction (Ministerul Apărării Naționale, 2008).

Initial facilities are defined as temporary and relocatable structures like tents, primarily used for short-term deployments in training, crisis, or conflict scenarios. These facilities, designed to be operational for no more than six months, offer basic, austere conditions suitable for rapid deployment. They provide essential shelter and workspaces but are limited in comfort and amenities.

Temporary facilities, also temporary and relocatable in nature, are intended for use in prolonged crisis or post-conflict situations. These structures are more durable than initial facilities, with a lifespan of up to 5 years. They offer improved living conditions, often including access to electricity, water, and sanitation. Technical solutions include tents with windbreaks and electrical installation or container construction with temporary foundations.

Permanent facilities represent the definitive, fixed constructions intended for long-term use. These buildings, which involve a significant engineering effort, are designed for special or representative functions within the military, such as MApN Headquarters. They are

[23] Approved by *Ordinul nr. M.91 din 12 septembrie 2008* and amended by *Dispoziția șefului Direcției domenii și infrastructuri nr. DDI-13 din 17 iunie 2022.*

built on state land with a focus on permanence, functionality, and design, reflecting a more substantial investment and a commitment to long-term usability.

Semi-permanent facilities are a new concept in the regulations of the Romanian military forces. This hybrid form of construction between the permanent structures and the temporary ones is usually a fixed building designed for use over a period extending beyond 5 years but not exceeding 25 years. These buildings should be isolated, not benefiting from the exceptions applied to temporary structures. Also, a key characteristic of these types is the built-in capability for space reconfiguration, redistribution, or partial reconstruction, with minimal expenses, enabling easy adaptation to future requirements.

Technical Solutions for Semi-Permanent Buildings

The lifespan of 25 years reflects the dynamic nature of military requirements rather than the technical capacity of the buildings, but the technical solutions used should relate to the building's duration of use to ensure cost-efficiency. In conclusion, brick or concrete structures do not represent a solution for these facilities. Instead, lightweight constructions with metal frameworks or load-bearing wooden walls are used (Guvernul României, 2004).

Steel Framing: Lightweight yet strong, steel frames provide a sturdy structure for buildings. They can be used with a variety of cladding materials to create durable and aesthetically pleasing structures. Using prefabricated panels for walls and roofing can significantly speed up the construction process. These panels, made from materials like wood, metal, or composites, provide good insulation and durability for permanent structures.

Figure no. 7. Light steel frame construction
(Light Steel Frame Association, 2022)

Wood structures: As buildings become more sustainable, timber becomes a popular solution due to its strength, appearance, and versatility. As structures grow larger, CLT (cross-laminated timber) has become a popular solution that can replace concrete and steel in modern construction. Another technical solution for wood buildings is timber frames, prefabricated or constructed on-site.

Figure no. 8. CLT prefabricated building
(Glulam, 2023)

When it comes to ensuring adaptability over time, the open plan offers an easy solution for interior modifications. Another solution that stands out as one of the most frequently employed strategies, is modular architecture (Schmidt 2016, p.20-27). Modules can be reconfigured, expanded, or relocated to suit changing needs. The design can meet intermodal transport standards without using a shipping container. Usually built as standardized room types can also be built to order by manufacturers who operate like indoor general contractors. Also, it can be produced in many parts of the world, at an industrial scale (Wallance 2021, p.36-42).

Figure no. 9. Modular building made of prefabricated 3D modules
(Smith, 2016)

Modular construction: This process involves the use of prefabricated modules that are assembled on-site offering a quicker construction process compared to traditional methods. Integrating essential components like wiring, plumbing, and insulation, and ensuring factory-based quality control contributes to the consistency and overall quality of the building.

Semi-permanent buildings in the military context

Although wooden barracks have been used since the beginning for the rapid construction of the Romanian military barracks, even being used after '89 due to their low costs, this type of construction was seen as a temporary solution. The majority of the military buildings in Romania is made of masonry due to the low cost of the material and the availability of cheap labor. Lightweight metal constructions have also been utilized, though with limited application, primarily for utilitarian structures such as warehouses, garages, or technical facilities. Due to advancements in construction technology, technical solutions for lightweight constructions provide similar comfort to permanent structures. Consequently, these semi-permanent constructions are increasingly utilized.

Aligning the national defense strategy towards alliance-based defense emphasizes the critical role of deployed forces, necessitating the establishment of a flexible and interoperable infrastructure. Integrating semi-permanent facilities into the real estate protocols of the Ministry of National Defense (MApN), drawing from collaborative missions and inspired by U.S. Army regulations, enables the development of modern, adaptable, and interoperable infrastructure. Therefore, conducting an analysis of U.S. military regulations regarding semi-permanent buildings is essential to gain a deeper understanding of the utilization of such buildings in a military context.

According to UFC 1-201-01 which outlines guidelines for non-permanent Department of Defense (DOD) facilities to support military operations, semi-permanent facility construction involves the buildings and facilities intended to serve a life expectancy of less than 10 years (120 months). However, through the maintenance and proper upkeep of essential building systems, it's possible to extend a facility's lifespan to 25 years (or 300 months). For these buildings, as well as for all types of non-permanent structures outlined in the instructions, there are standardized designs available. These designs are versatile, catering to various site conditions, missions, and other factors. It is recommended to utilize these standardized designs whenever they meet the project requirements before starting the design of a unique non-permanent facility.

As part of the US Army Corps of Engineers (USACE), Centers of Standardization (COS) have been established to focus on standard design development. These centers develop and maintain standard designs, criteria, and Unified Facilities Criteria (UFCs) in collaboration with relevant stakeholders. Additionally, they provide consultation services to districts involved in design and construction and document lessons learned for continuous improvement (U.S. ARMY CORPS OF ENGINEERS, 2006). The COS employs a web-based platform to disseminate pertinent information regarding the MILCON Business Process (MBP) and the development of standard designs. This resource provides comprehensive details, including contact information for all COS and USACE Headquarters, insights into standard facility specifications such as Army Standards and Designs, as well as 1391 Templates. Additionally, users can access COS policy documents and essential links to further COS and MBP-related resources.

The Center of Standardization (COS) for Nonpermanent Facilities plays a key role in developing and reviewing Army designs for temporary and semi-permanent facilities, as guided by UFC 1-201-01. Their work includes developing standardized designs for efficient base camp layouts. This is part of their broader role in establishing Joint/Army design standards and serving as the Army's primary design agent for temporary and semi-permanent facilities, ensuring practical and adaptable military construction solutions. They focus on conceptualizing and creating functional, adaptable spaces within standardized exteriors, emphasizing the use of local materials, minimizing heavy equipment and maintenance needs, avoiding fire sprinklers, and eliminating load-bearing interior walls, thereby ensuring practicality and efficiency in military construction.

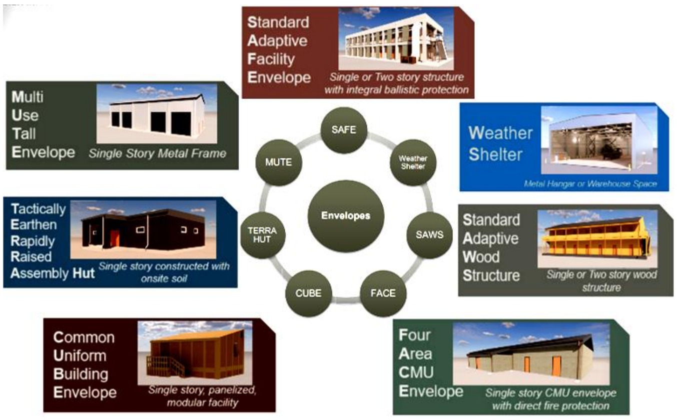

Standard
Adaptive
Facility
Envelope
Single or Two story structure with integral ballistic protection
Multi
Use
Tall
Envelope
Single Story Metal Frame
Weather
Shelter
Metal Hangar or Warehouse Space
Tactically
Earthen
Rapidly
Raised
Assembly Hut
Single story constructed with onsite soil
Standard
Adaptive
Wood
Structure
Single or Two story wood structure
Common
Uniform
Building
Envelope
Single story, panelized, modular facility
Four
Area
CMU
Envelope
Single story CMU envelope with direct fire protection
SAFE
MUTE
Weather Shelter
Envelopes
TERRA HUT
SAWS
CUBE
FACE

Figure no. 10. Envelope types developed by COS for adaptable non-permanent facilities (Engineer Research and Development Center (ERDC), 2024)

The standard envelopes for semi-permanent buildings developed by COS include various designs for temporary and semi-permanent buildings. Standard designs are available for execution in any envelope, providing an interior layout ready to use for operations, life support, or services.

SAFE is a concrete frame structure measuring 12.9m x 34.3m, covering an area of 885m². This two-story structure offers flexibility in length, allowing modifications by standard bay lengths. Its adaptable design makes it a practical choice for various functions such as Billeting, Administrative spaces, Operations, and Life Support Facilities. The single-story version with an area of 442,5 m^2 is another great choice for Billeting, Administrative spaces, Operations, and Dining.

MUTE is a modular structure, a single-story building with a metal frame, spanning 12.8m by 30.5m, and offering a total area of 390m². Available in two height options, 4m, and 6m, its metal envelope design allows for length adjustments using standard bay increments. MUTE is highly suitable for purposes like Storage, Maintenance, or Fire Station and Supporting Facilities, offering technical adaptability and space efficiency.

SAWS is a wooden structure with concrete foundations, offered in sizes of 442.5m² for a single story and 885m² for two stories. Their wood construction allows for easy modification in length using standard bay lengths. These structures are particularly suited for Billeting, Administrative Spaces, and Operations, offering flexibility in design.

In summary, COS's standard envelopes for semi-permanent structures like SAFE, MUTE, and SAWS, exemplify the integration of adaptability, efficiency, and functionality. These designs cater to a variety of military needs, offering customizable layouts and dimensions, allowing for the facilities to be effectively utilized for operations, life support, or service activities. An essential element worth examining in this design approach is the adoption of standard project types. This methodology facilitates uniformity and efficiency, particularly important in military constructions where adaptability and quick deployment are crucial.

III. Shortening the Construction Project Life Cycle – Standardized Projects

A standardized project or blueprint is designed for repeated use in the construction of multiple objectives of a similar nature. These predefined templates reduce the time and complexity typically involved in starting from scratch, allowing for quicker mobilization and execution of plans. This approach not only accelerates the project's implementation but also ensures consistency and adherence to best practices, making it an invaluable strategy in time-sensitive situations like military activity.

In project development, a structured approach is crucial, as demonstrated by the OAR (Ordinul Arhitecților din România) *Misiunile arhitectului*. This framework outlines distinct stages that guide the project from inception to completion. The phases typically include:

1. **Preliminary Stage:** Establishing initial project data and configuring the design process.
2. **Preparatory Stage:** Setting the main parameters of the real estate investment in relation to the site.
3. **Concept:** Configuring construction functionally and aesthetically.
4. **Final Project:** Establishing all construction components and validating them.
5. **Authorization Project:** Designing for authorization and estimating construction costs.
6. **Tendering Project:** Finalizing technical design and coordination.
7. **Execution Project:** Conducting detailed design and coordination of projects.
8. **Consultancy in Selection of Construction Works:** Organizing tender documentation and selecting contractors.
9. **Execution Assistance:** Supervising work execution and providing technical assistance.
10. **Monitoring of Building Behavior in Operation and Intervention Over Time:** Monitoring construction operation and intervening as necessary.

This structured framework ensures thorough planning, execution, and monitoring of each phase, leading to more efficient and effective project delivery.

Standardized projects significantly shorten or even eliminate certain stages of project realization due to their predefined nature and streamlined processes. For instance, in the Preliminary Stage, standardized projects provide predefined objectives and requirements, minimizing the need for extensive initial planning. Similarly, in the Concept Stage, pre-designed concepts offered by standardized projects eliminate the need for multiple design iterations, thereby expediting the process of configuring construction functionally and aesthetically. Moreover, in the Tendering Project Stage, standardized projects streamline the process by providing organized tender documentation, thus reducing the time and effort required for selecting contractors. Additionally, prefabricated construction methods associated with standardized projects accelerate the Execution Project Stage, as components are produced off-site and assembled faster on-site. This approach allows for quicker mobilization and execution of plans, leading to a more efficient project implementation process overall, while also reducing both the time and costs associated with the project.

In conclusion, the use of standardized projects is crucial for a swift and efficient construction process. These designs not only streamline the construction phases but also ensure consistency in quality and optimize resource utilization. In the context of prefabricated and lightweight constructions, standardized projects are key to rapid deployment and adaptability, essential for responding to evolving requirements and operational challenges.

IV. Regulatory Framework for Semi-Permanent Facilities

The efforts to harmonize Romanian military regulations with international counterparts have resulted in some inconsistencies with existing national construction laws. Because military buildings are subject to both military-specific regulations and national construction laws, a clear understanding of military construction requires comprehending the legal framework and understanding the impact of the building's operational duration and expected lifespan.

The expected duration of use indicates the period over which a fixed asset's initial value is recovered fiscally through depreciation. It often falls short of the asset's actual physical lifespan, but the depreciation of the investment is mandatory in order to decommission a building.

The classification of military facilities into four categories introduced in 2008 in *Regulamentul proprietății imobiliare în Ministerul Apărării Naționale* is a clear intention to modernize the approach of infrastructure and it helps clarify the expected usage durations of buildings in a military context. Nevertheless, the operating duration of MApN infrastructure stipulated in *Normele tehnice de domenii şi infrastructuri*[24] and *Normele tehnice pentru lucrări de întreținere și reparații curente la clădirile şi construcțiile speciale din patrimoniul imobiliar al Ministerului Apărării*[25] brings the military standard in alignment with the civil construction regulation. Accordingly military buildings should have a useful lifespan estimated at maximum duration specified in the *Catalogul privind clasificarea și duratele normale de funcționare a mijloacelor fixe* approved *by Hotărârea Guvernului nr. 2.139 din 30 noiembrie 2004*.

The system presented in the *Catalog* prioritizes a facility's functional performance and does not specify a distinct lifetime for semi-permanent facilities. Consequently, semi-permanent buildings are accounted for and depreciated in the same manner as permanent constructions, with the depreciation rate being determined based on the building's intended use. For instance, administrative buildings, regardless of their construction approach, are expected to have a normal operating life ranging from 40 to 60 years. Therefore, any military headquarters, even those labeled as temporary or semi-permanent, are anticipated to remain operational for at least 40 years to ensure depreciation prior to their decommissioning. This scenario highlights a mismatch between the fixed assets' operational durations and the specific needs of the military infrastructure.

The requirements and the flexibility demanded by military infrastructure are not reflected in the classification system of *Hotărârea Guvernului nr. 2.139 din 30 noiembrie 2004* but this regulation specifies that for the assets related to national defense, the MApN, with approval from the Ministry of Public Finance, may set its own criteria for classification and operational periods.

In conclusion, in order to use semi-permanent buildings as intended in *Regulamentului proprietății imobiliare în Ministerul Apărării Naționale*, naming to respond swiftly to a mid-

[24] Approved by *Dispoziția șefului Direcției domenii și infrastructuri nr. DDI-12 din 2022*

[25] Approved by *Dispoziția șefului Direcției domenii și infrastructuri nr. DDI-4 din 14 aprilie 2020*

term requirement and allow for site remodeling by decomisionig the buildings after just 10 or 25 years, under the national law that allows MApN to establish its own norms, it is essential to develop specifications for the design and eventual decommissioning of these semi-permanent structures that align with both the strategic objectives of the Ministry of National Defense (MApN) and the overarching national regulations.

We appreciate that the introduction of a new class of operational duration for semi-permanent military facilities within the framework of the existing military norms will contribute to greater efficiency of military infrastructure use. This proposed classification named *Adaptable Military Constructions*, underlining the inherent flexibility and functionality of these structures within a significant yet finite timeframe, would anticipate a duration of use of 10 to 25 years. This approach allows for the development of military infrastructure in a more efficient and adaptable manner for future needs.

Conclusions

The implementation of real estate investments in the military sector, a process often marked by high costs, time constraints, and the need to navigate complex legislative and departmental regulations, can greatly benefit from using semi-permanent facilities.

Advantages of utilizing semi-permanent structures

In exploring the advantages of semi-permanent military structures, several key benefits stand out. These structures offer a dynamic solution to the evolving needs of modern military operations, combining efficiency, adaptability, and sustainability. Key advantages include:

1. **Rapid Deployment**: Semi-permanent structures can be rapidly constructed, often within days to weeks. This speed is crucial in urgent scenarios where quick setup is essential for operational readiness.
2. **Cost-Efficiency**: Building traditional, permanent military facilities for short- to mid-term use can be prohibitively expensive. Semi-permanent structures provide a more economical option, allowing military budgets to be allocated more towards operational and logistical needs rather than infrastructural expenses.
3. **Versatility and Adaptability**: These structures are highly adaptable to various military needs, covering a wide range of space types. They can be customized for different purposes, including barracks, command centers, medical facilities, storage areas, or operational headquarters.
4. **Environmental Sustainability**: The prefabrication of these structures significantly reduces environmental impact. This is achieved through minimized waste and efficient use of construction materials. Often designed with sustainability in mind, they typically utilize recyclable materials, reducing the ecological footprint of military operations, especially in environmentally sensitive areas.
5. **Minimal Operational Disruption**: Implementing semi-permanent structures, whether for renovations, supplementing overcrowded facilities, or developing new sites, minimizes disruption to ongoing operations. This ensures that military personnel can maintain their focus and effectiveness without significant interruptions to their activities.
6. **Long-Term Durability**: Despite often appearing temporary, these structures are built for robustness and extended use. Their durability ensures they can serve military purposes for several years, providing a reliable mid-term solution and potentially longer with proper maintenance.

Charting Future Paths: Key Conclusions and Insights

In the ever-evolving landscape of military operations, the dynamic nature of contemporary combat and defense strategies necessitates a flexible approach to infrastructure development. The inherent volatility of military contexts often renders the function of a building obsolete, while simultaneously, emerging needs remain unaddressed by existing infrastructures. In this regard, the modification of a building's purpose often entails costly and time-consuming technical alterations. Thus, the adoption of adaptable semi-permanent military constructions emerges as a pragmatic solution. These structures are inherently designed for easy adaptation to various functional typologies, ensuring technical feasibility for timely modifications, while also substantially reducing the time and technical documentation required.

To capitalize on the benefits of adaptable semi-permanent buildings in military contexts, a key strategy involves their initial design with flexibility in mind, enabling easy modification for diverse functions. These buildings are constructed following a standardized plan, which encompasses various interior layout options tailored to specific intended uses. This approach facilitates the swift adaptation of structures to meet changing operational needs. In aligning with this adaptability, the duration of use should be determined based on the materials employed in construction, not as it is now by function. By setting the lifespan of these buildings in accordance with the durability of their materials, the military can effectively balance the need for flexibility with the sustainability and practicality of the construction, ensuring that these adaptable structures serve their purpose efficiently throughout their intended lifecycle.

In summary, the strategic incorporation of 'Adaptable Military Constructions' into the military real estate portfolio initiates a period of dynamic and efficient infrastructure development. Enhanced by standardized projects for semi-permanent facilities, this approach equips the Ministry of National Defense to effectively address cost, time, and regulatory challenges, establishing a new standard in military infrastructure development.

BIBLIOGRAPHY:

1. Bărbulescu, G., Pădureanu, S., & Alistar, C. (1996). *Istoria activității de proiectare a construcțiilor militare.* București: Editura Curtea Veche.
2. Departamentul Apărării al Statelor Unite ale Americii. (2022). *Facilități nepermanente ale DOD în sprijinul operațiilor militare.* UFC 1-201-01. Preluat de pe https://www.wbdg.org/FFC/DOD/UFC/ufc_1_201_01_2022_c4.pdf
3. Direcția domenii și infrastructuri. (2020). *Dispoziția șefului Direcției domenii și infrastructuri nr. DDI-4 din 14 aprilie 2020 pentru aprobarea Normelor tehnice pentru lucrări de întreținere și reparații curente la clădirile și construcțiile speciale din din patrimoniul imobiliar al Ministerului.* Accesat prin aplicația Lexmil din rețeaua INTRAMAN la 17 martie 2023.
4. Direcția domenii și infrastructuri. (2022). *Dispoziția nr. DDI-13 din 17 iunie 2022 pentru aprobarea Regulamentului proprietății imobiliare în Ministerul Apărării Naționale.* Accesat prin aplicația Lexmil din rețeaua INTRAMAN la 17 martie 2023.
5. Direcția domenii și infrastructuri. (2022). *Dispoziția șefului Direcției domenii și infrastructuri nr. DDI-12 din 13 aprilie 2022 pentru aprobarea Normelor tehnice de domenii și infrastructuri.* Accesat prin aplicația Lexmil din rețeaua INTRAMAN la 17 martie 2023.
6. Engineer Research and Development Center (ERDC). (2024, May 2). *CoS FOR NON-PERMANENT FACILITIES.* Preluat de pe MILCON Requirements, Standardization, and Integration (MRSI): https://rfpwizard.mrsi.erdc.dren.mil/MRSI/content/cos/tam/center_home_page/Library/COS%20Facility%20Overview%20-%20%20February%202024.pdf

7. Engineer Research and Development Center (ERDC). (fără an). *About TAM: The Center of Standardization (CoS) for Nonpermanent Facilities*. Preluat de pe MILCON Requirements, Standardization, and Integration (MRSI): https://mrsi.erdc.dren.mil/cos/
8. Engineer Research and Development Center (ERDC). (fără an). *ENVELOPES*. Preluat de pe MILCON Requirements, Standardization, and Integration (MRSI): https://mrsi.erdc.dren.mil/cos/tam/envelopes/
9. Glulam. (2023, Decembrie 11). GLULAM SA: Prima fabrica de CLT din Romania, la Targoviste. (S. P. Edit, Ed.) *Revista construcțiilor*(209), pg. 10-11. Preluat de pe Revista construcțiilor: https://www.revistaconstructiilor.eu/wp-content/uploads/2023/12/rc_nr_209_decembrie_2023.pdf
10. Guvernul României. (2004). *Hotărârea nr. 2.139 din 30 noiembrie 2004 pentru aprobarea Catalogului privind clasificarea și duratele normale de funcționare a mijloacelor fixe.* Publicat]n Monitorul Oficial nr. 46 din 13 ianuarie 2005. Preluat de pe https://legislatie.just.ro/Public/DetaliiDocumentAfis/58613
11. Herjeu, C. (1902). *Istoria Armei Geniului.* București: I.V. Socecu.
12. Light Steel Frame Association. (2022, November). The latest in Light Steel Framing Technology Development. *Light Steel Framing Magazine*(6), pg. 4-6. Preluat de pe https://issuu.com/radarcommunications/docs/lsf_mag_autumn_22_issue_6_online
13. Ministerul Apărării Naționale. (2007). *Strategia de transformare a armatei României.* București. Preluat de pe https://drpcvp.mapn.ro/webroot/fileslib/upload/files/PROGRAME%20SI%20STRATEGII/STRATEGIA_TRANSFORMARE_ARMATA_ROMANIEI.pdf
14. Ministerul Apărării Naționale. (2008). *Ordinul nr. M. 45 din 9 mai 2008 pentru aprobarea Normelor tehnice de domenii și infrastructuri.* Publicat în Monitorul Oficial nr. 405 din 29 mai 2008. Preluat de pe https://legislatie.just.ro/ Public/DetaliiDocumentAfis/93541
15. Ministerul Apărării Naționale. (2008). *Ordinul nr. M.44 din 9 mai 2008 privind aprobarea Normelor tehnice pentru lucrări de întreținere și reparații curente la clădirile și construcțiile speciale din patrimoniul imobiliar al Ministerului Apărării.* Publicat]n Monitorul Oficial nr. 402 din 28 mai 2008. Preluat de pe https://legislatie.just.ro/public/DetaliiDocument/93499
16. Ministerul Apărării Naționale. (2008). *Ordinul nr. M.91 din 12 septembrie 2008 privind aprobarea Regulamentului proprietății imobiliare în Ministerul Apărării.* Publicat]n Monitorul Oficial nr. 668 din 26 septembrie 2008. Preluat de pe https://legislatie.just.ro/Public/DetaliiDocument/97630
17. Ministerul Apărării Naționale. (2013). *Ordinul nr. M 92 din 16 septembrie 2013 privind aprobarea Instrucțiunilor pentru scoaterea din funcțiune și casarea activelor fixe, precum și declasarea și casarea bunurilor materiale, altele decât activele fixe, în cadrul Ministerului Apărării Naționale.* Preluat de pe https://legislatie.just.ro/Public/DetaliiDocument/151635
18. Ministerul Apărării Naționale. (2021). *Strategia militară a României.* București. Preluat de pe https://sgg.gov.ro/1/wp-content/uploads/2021/08/STRATEGIA-MILITARA-A-ROMANIEI-1.pdf
19. Ministerul Dezvoltării, Lucrărilor Publice și Administrației. (fără an). *Normativ privind executarea lucrărilor de întreținere și reparații la clădiri și construcții speciale GE 032-97.* Preluat pe ianuarie 15, 2004, de pe https://www.mdlpa.ro/pages/reglementare22
20. OAR (Ordinul Arhitectilor din România). (2014, Iunie). *Misiunile arhitectului.* Preluat de pe Ordinul Arhitectilor din România: https://oar.archi/wp-content/uploads/2021/02/misiunile_arhitectului_web_pdf_1462749114-1.pdf
21. Petrișor, A. (2011). *FATE - Conversia fostelor baze militare în centre antreprenoriale. O perspectiva românească.* București: Editura Ars Docendi.

22. Schmidt, R., & Austin, S. (2016). *Adaptable Architecture – Theory and Practice.* New York: Routledge.
23. Smith, R. E. (2016, September 8). *Off-Site And Modular Construction Explained*. Preluat de pe WBDG (Whole Building Design Guide): https://www.wbdg.org/resources/site-and-modular-construction-explained
24. Târzioru, M., & Pădureanu, S. (1995). *Istoria construcțiilor și domeniilor militare.* București: Editura Militară.
25. U.S. ARMY CORPS OF ENGINEERS. (2006, March). *About the Centers of Standardization.* Preluat de pe MILCON Requirements, Standardization, and Integration (MRSI): https://rfpwizard.mrsi.erdc.dren.mil/MRSI/content/cos/ cos_home_page/Library/ memo-realignment-establishment_of_cos-mar06.pdf
26. Wallance, D. (2021). *The Future of Modular Architecture.* New York: Routledge.

1053477-3045-1396-24-40

SMART CRITICAL INFRASTRUCTURES IN THE WORLD'S CITIES: AN ESSENTIAL STEP FOR THE QUALITY OF LIFE

Miruna-Alexandra CIOSU
Second lieutenant, "Carol I" National Defense University, Bucharest, Romania
E-mail: mirunaciosu@yahoo.com

Abstract: *Critical infrastructure is the backbone of our economy, security, and societal well-being. We rely on critical infrastructure when we turn on the lights at home, drink water, travel using transportation, or use any means of communication. Urbanization, globalization, and the interdependence of physical and digital infrastructures have a significant impact on our economy and society, leading to the design of smart cities. Therefore, safe, efficient, sustainable, and resilient infrastructure is essential for maintaining a high quality of life. In this article, the aim is to highlight the impact of critical infrastructure on the quality of life. The main objective of the article is to inform the public about the importance of investing in and efficiently managing critical infrastructure to ensure access to essential services, resilience in emergency situations, innovation through cutting-edge infrastructure technologies, and contribution to sustainable development.*
Keywords: *critical infrastructures; quality of life; sustainability; durability*.

1. Preliminary Considerations

Human history has been written over centuries in the rhythm of changes, almost always forced, which have led the various types of societies that have inhabited and continue to inhabit the planet, constantly evolving. We, as humans, have always adapted to new realities with a single final objective beyond even our well-being: our survival.

The purpose of this article is to highlight the impact of critical infrastructures on the quality of life. These infrastructures play an essential role in supporting a functional society and improving the well-being of its inhabitants. The main objective of the article is to inform the public about the importance of investing in and efficiently managing critical infrastructures to ensure access to essential services, resilience to emergency situations, innovation through cutting-edge infrastructure technologies, and contribution to sustainable development. It emphasizes that adequate infrastructure is necessary to overcome the challenges faced by the cities of the world regarding the decent living standards of their inhabitants, as well as meeting the requirements of export markets and how this factor can help strengthen the economy of a developing city.

Critical infrastructure represents the backbone of modern society, and it is in direct interaction with the infrastructure sectors that determine our evolution or involution as inhabitants. In addition to the direct physical damages that can be caused by extreme weather and climate phenomena, such as heatwaves, heavy rainfall, and floods, there are also other indirect damages caused by the loss of functionality or interruptions in supply chains or auxiliary services (Naturklima 2022, 5). Moreover, the impact on these infrastructures involves high economic costs for the territory.

Territorial infrastructure plays a crucial role in the cost of living and the functioning of critical infrastructures. These primarily refer to transportation, energy, communications, and water networks that support the development and well-being of a region. The Ministry of Environment represents one of the government institutions that holds an important role in managing and planning territorial infrastructure to ensure sustainable and high-quality development.

Currently, people pay special attention to examining the quality of life due to current economic challenges and the high cost of living. Although the annual investment plan at the national level is ensured in terms of government attention and expenditure, ensuring the quality of life in the medium and long term depends on investments in appropriate infrastructure.

As society continues towards a more welfare-centered modern mentality, the quality of life that infrastructure can improve is currently at the forefront due to its importance. By analyzing the old infrastructure, it can no longer serve the new requirements of the community, leading to the reconsideration of infrastructure planning and, at the same time, focusing on resilience.

On the other hand, an important factor in maintaining stability and security is the protection of critical infrastructures, which requires increased involvement of key international actors such as states and international organizations in adjusting and developing strategies in the field (Romanian Intelligence Service, Critical Infrastructure Protection, 5). At the same time, these strategies should ensure risk monitoring and warning systems, as well as adopting or promoting prevention or countermeasures efforts against threats.

Additionally, terrorist threats have been a key moment for the international community to expand the concept of *"critical infrastructure"* worldwide and adopt uniform integrated measures in national and regional protection strategies (Tsuyoshi Takano *et al*. 2023, 100).

Similarly, the sense of values and lifestyle of citizens can be drastically influenced by natural disasters, pandemics, or economic crises. Therefore, infrastructure should be considered not only as an asset but also as a tool for providing services that improve quality of life and social inclusion, as well as addressing this concept from a comprehensive and multidisciplinary perspective.

2. Several Conceptual Delimitations

For the analysis of quality of life and critical infrastructure, it is necessary, first and foremost, to establish some conceptual delimitations because the international specialized literature records a wide variety of theoretical formulations, especially regarding the modern welfare-centered mentality, which is largely influenced by infrastructure. Thus, we bring to attention concepts from both Romanian and international literature.

Critical infrastructure represents an asset or system essential for maintaining the vital functions of society. Damage to critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activities, or malicious behavior can have a significantly negative impact on the EU's security and the well-being of its citizens.

The concept of quality represents monitoring of a logical process, from measurements to obtaining certifications regarding the quality of a service and meeting the objectives of each critical infrastructure that plays a vital role in quality of life. These certifications can take the form of a quality seal representing a guarantee in facilitating the needs of residents, leading to reliable quality.

Meanwhile, quality of life has been defined as a set of desirable things not always recognized by the market, which, like sustainability, has economic, social, and environmental dimensions (Inés Sánchez de Madariag 2004, 102).

Quality of life usually captures how happy or satisfied people are in their lives. It encompasses a complex and interacting set of factors operating at different scales, from individuals to communities and countries, and can be measured objectively and subjectively.

In the same vein, the quality of life method (QOL/Quality of life) measures an individual's happiness in relation to social issues and facilitates the evaluation of investments in transport infrastructure with a performance-based evaluation system (Yoshitsugu, Hayashi *et al.* 2023, 17).

At the same time, the use of the terms *"sustainability"* and *"sustainable"* may seem ambiguous in the context of the urgent and necessary global concern for environmental protection, and in the various initiatives undertaken by governments and private entities, they have different characteristics.

Sustainable development, in turn, has been defined as meeting the needs of the present without compromising the ability of future generations to meet their own needs, integrating environmental, social, and economic considerations into decision-making processes. The characteristics of sustainable development are presented in Figure no. 1.

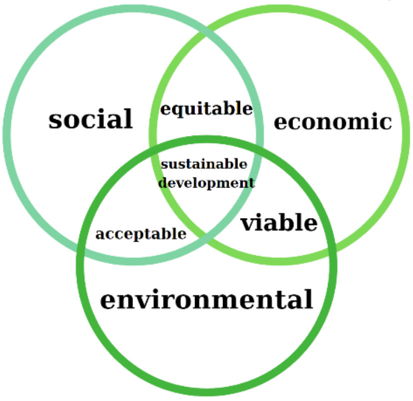


Figure no. 1. Characteristics of sustainable development
Source: https://www.renovablesverdes.com/ro/sustentabilidad-y-sostenibilidad/, accessed 15 Dec. 2023

The Spanish dictionary defines *"sustainability"* as *"a process"* whose main objective is to find a balance between the environment and the use of natural resources. Over time, humanity has degraded natural resources in such a way that it is now necessary to search and plan with a sense of responsibility for their consumption to guarantee the existence of future society.

Therefore, sustainability seeks for the next generation to find a world and a society that are at least as good, if not better, than they are now. Meanwhile, sustainable development is based on three areas: society and people, economy, and planet. These represent the main characteristics that a society must have to achieve sustainable development.

On the other hand, sustainable infrastructure represents quality infrastructure that places a greater emphasis on the economic and engineering qualities of a project, such as focusing on innovative technologies (Daniel, Taras. 2019).

Thus, critical infrastructures and sustainable development are two interconnected aspects of modern society, closely related in efforts to create a more resilient and sustainable environment. The combination of well-managed critical infrastructures and environmentally and resource-oriented sustainable development can bring long-term benefits to society.

3. The research methodology

In writing the article, a qualitative method was used, which consisted of gathering multiple sources and analyzing them regarding the focus on critical infrastructures, aiming to highlight the importance of quality of life and how it can be enhanced through investments in critical infrastructure. Additionally, the research methodology is based on the analysis of existing literature and expertise in the fields of critical infrastructure, sustainability, and economic efficiency.

This method involved identifying and selecting reliable and relevant sources in the areas under consideration, such as reports from international organizations, academic studies, and resources published by experts. Subsequently, a thorough reading and understanding of these sources was conducted to extract relevant concepts and principles related to critical infrastructure, economic efficiency, and sustainability.

The information was synthesized in a concise and clear format, highlighting key lessons and relevant conclusions. An analytical and synthetic approach to the literature and expertise in the field of critical infrastructure emphasized the identification and extraction of relevant quality lessons and practices to improve critical infrastructure and quality of life in communities.

4. Direct Proportionality between Critical Infrastructures and Quality of Life

There is a direct proportionality between critical infrastructures and quality of life in society. Critical infrastructures, which include essential systems and facilities for the daily functioning of a community, play a vital role in determining the level of comfort, safety, and well-being of the inhabitants.

According to most (inter)national studies, life satisfaction in small towns is higher than in other types of cities with more inhabitants (Gareis, Philipp *et al.* 2021, 39*)*. The population of small towns in central locations seems to benefit from the infrastructure of neighboring cities and elsewhere. Somehow, they are very satisfied with the way they live, despite a low level of satisfaction with infrastructure.

When it comes to the quality of critical infrastructure, authorities must ensure at least access to informational technical standards and regulations to guarantee reliable measurements and establish a system that allows accreditation of entities so that their results are accepted internationally, not just nationally (Clemens Sanetra and Rocío M. Marbán 2020). Additionally, quality critical infrastructure is also an essential factor in supporting local businesses, resulting from a high quality of life for residents, as well as economic growth in the respective city.

For greater clarity regarding the direct proportionality between critical infrastructures and quality of life, an example relevant to the subject is discussed, from which several essential conclusions can be drawn.

Experts estimate that by 2040, 65% of the world's population will live in cities (Jayna Locke 2023). This means much more emissions, water and energy consumption, as well as waste. Thanks to a combination of smart technologies, such as sensors, wireless networks, and communication devices, cities can develop comprehensive smart systems to automate, manage, and optimize important urban services and utilities.

Let us start with the question *"What is a smart city?"*. The most technologically advanced cities have something in common: they use technology to provide the best and most services to citizens, leading to their well-being. Increasingly, smart cities also include initiatives that improve sustainability through environmental monitoring and energy and water-saving devices, as well as the use of renewable energy solutions.

When Paris was created, it was not intended to be a metropolis. However, over time, the city has had to remodel its critical infrastructure several times to keep pace with technological changes. One of the reasons Paris is called the *"City of Light"* is not because of its nightlife, but rather because it was one of the first European cities to install gas street lighting. Today, Paris resembles many other cities in its acknowledgment that it must adapt to new technologies to continue to be a modern city.

Quoting Stefano Puntoni, a marketing professor, he believes that technology not only reflects our identity but also shapes it (Gizem Yalcin and Stefano, Puntoni 2023). This is why critical infrastructures should adapt to new innovations because the human brain operates in conjunction with these changes, being somewhat incompatible with old infrastructures and mentalities, thus creating gaps in society.

Infrastructure, which people often consider self-evident, together with technology and innovation, can lead to quality of life. This can be illustrated with two examples that initially seem simple and insignificant: parking and electric vehicle charging (Alexander Soley 2021).

Parking in urban areas is a major problem. Parisian drivers spend an average of 20 minutes finding a parking spot once they reach their destination. During that time, precious energy and time are wasted. As long as vehicles remain an important part of modern transportation, infrastructure solutions for building parking lots are necessary.

Many forget that the first *"horseless carriages"* ran on steam, gas, and electricity. At the same time, gasoline-powered cars predominated due to lower prices and better energy infrastructure. Now that EVs are *"back"*, the establishment of EV charging networks is necessary.

Street charging stations are important for cities because electric vehicles are not practical if you do not live close to a charging station, and accessing the charging station can be difficult. Some governments have mandated and already provided financial incentives to ensure that a percentage of parking spaces include chargers for electric vehicles.

Unlike the seemingly laissez-faire American approach, the European Union (EU), Norway, Switzerland, and the United Kingdom have mandated that public fast chargers for direct current have CCS plugs, thus establishing a standard through regulations. This illustrates that regulation can successfully set standards and provide efficient infrastructure for users.

Therefore, autonomous vehicles will have fewer decisions to make if there are fewer standards for electric vehicle charging and parking space availability is updated in real-time. One of the primary objectives of smart cities is to improve someone's quality of life, and eliminating complications such as finding parking spaces and compatible charging stations is just one example of what smart cities can do. By developing uninterrupted smart infrastructure, we can be closer to a more promising future.

5. Evaluation of risks and preparation of counter measures against possible threats

Risk assessment and preparation of counter measures against threats related to critical infrastructures are crucial processes to ensure the safety and stability of communities, thereby contributing to maintaining and improving quality of life.

Risk management refers to the probability of an unfavorable event occurring. It differs from vulnerabilities, which speak to the likelihood that the system can be exploited when a risk materializes.

In this sense, risk management involves implementing preventive or detection controls so that these risks can be stopped before they occur.

Approaching disasters or issues, whether directly related to climate change or not, requires governance that applies multisectoral risk management and is not limited to national emergency response agencies (Alicia Bárcena *et. al*. 2021, 9).

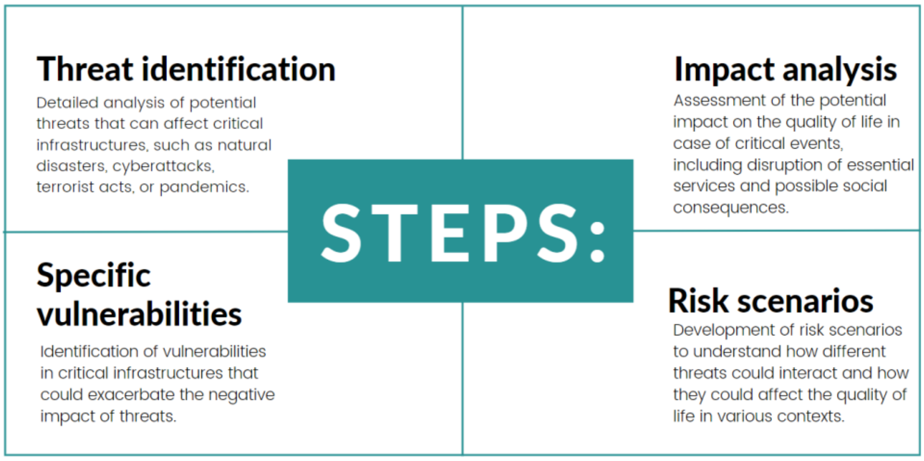
In this context, risk management must include the generation of response and adaptability capacities in the various stages of development of different natural or man-made problems, aiming to articulate permanent and emergency policies in different sectors and levels of governance (Alicia Bárcena *et. al*. 2021, 9). Risk management regarding natural disasters also requires a social protection component, complementary to the adaptation of production processes and public and private infrastructure, ecosystem protection, territorial planning, and sustainable financing (Alicia Bárcena *et. al*. 2021, 9).

Currently, our society exceeds planetary boundaries. The current crisis is a wake-up call for our planet and a call to action for our policies, for a transformative recovery that places equality at the center and moves towards sustainable development, without leaving anyone behind.

Social protection systems are essential for promoting inclusion and guaranteeing the exercise of economic, social, and cultural rights, as well as for favorable critical infrastructure (Alicia Bárcena *et. al*. 2021, 119). Additionally, they are essential for building social and fiscal pacts that provide sustainability for our societies and contribute to achieving a transformative recovery concerning the choice of critical infrastructure leading to citizens' welfare.

It is imperative that social protection systems be designed in an articulated manner with disaster management policy as a whole. This must be done primarily in terms of the role these systems play in the face of recurring crises and in the idea of achieving a transformative recovery that promotes equality and economic and productive reactivation within a sustainable environment. This involves strengthening links with sectoral and social promotion policies and directing towards the full consolidation of welfare in which society and inclusive and sustainable social development in all its dimensions are valued and prioritized, with social protection as a central instrument (Alicia Bárcena *et. al*. 2021, 119).

In the same vein, risk assessment involves several stages and is presented in Figure No. 2:



STEPS:

Threat identification

Detailed analysis of potential threats that can affect critical infrastructures, such as natural disasters, cyberattacks, terrorist acts, or pandemics.

Impact analysis

Assessment of the potential impact on the quality of life in case of critical events, including disruption of essential services and possible social consequences.

Specific vulnerabilities

Identification of vulnerabilities in critical infrastructures that could exacerbate the negative impact of threats.

Risk scenarios

Development of risk scenarios to understand how different threats could interact and how they could affect the quality of life in various contexts.

Figure no. 2. Stages of risk assessment
Source: Julian, Guillermo 2022, 32.

Holistic solutions are the specific solution for risk management of critical infrastructures that undoubtedly require appropriate security products and services for risks, threats and vulnerabilities (Manuel Sánchez Gómez-Merelo 2018, 14).

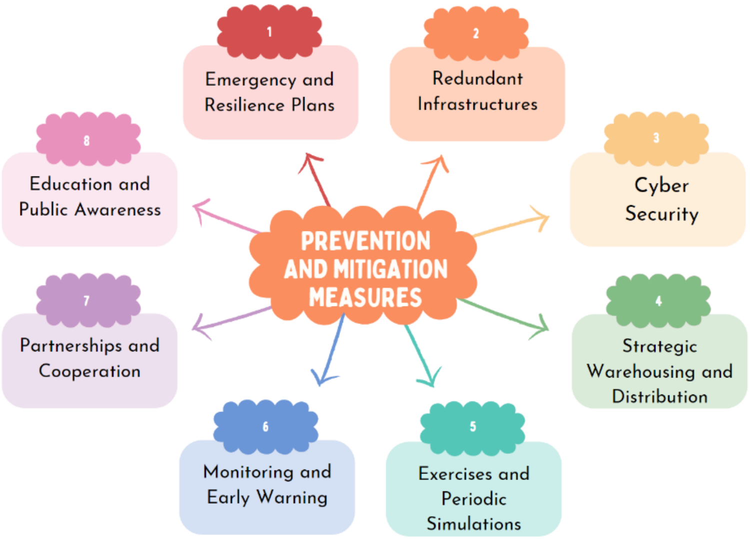

1
Emergency and Resilience Plans
2
Redundant Infrastructures
3
Cyber Security
4
Strategic Warehousing and Distribution
5
Exercises and Periodic Simulations
6
Monitoring and Early Warning
7
Partnerships and Cooperation
8
Education and Public Awareness
PREVENTION AND MITIGATION MEASURES

Figure no. 3. Prevention and Mitigation Measures
Source: National Road Safety Strategy.

By implementing these counter measures and continuously assessing risks, the resilience of critical infrastructures can be improved, contributing to maintaining and enhancing the quality of life in communities. It is essential to have an integrated and collaborative approach to address challenges and ensure a safe and sustainable environment for residents.

6. Methods of enhancing the quality of life through critical infrastructures

Improving quality of life through critical infrastructure involves developing, managing, and optimizing these infrastructures to meet the essential needs of the community.

Experts have recommended a series of approaches to improve and ensure the implementation of best practices in infrastructure planning, design, construction, and operation:

a) Providing incentives to support the development and application of best practices.
b) Improving environmental impact assessment, both in terms of rigorously analyzing alternatives to ensure that the proposed infrastructure solution is the best option, and in enhancing mechanisms for environmental and social management control within regulatory agencies.
c) Enhancing practices and planning in the decision-making process regarding infrastructure development.
d) Making project information public, as an informed public is also essential to drive the changes we need to see in infrastructure planning and best practices. This way, we can improve understanding of specific actions that contribute to sustainability, ensure social justice, and enhance transparency and accountability.
e) Understanding the long-term costs and benefits of infrastructure, both economically (and not just financially) and socially and culturally.

Smart cities have the function of optimizing city functions, improving the quality of life of citizens, and even promoting economic growth through the use of intelligent technologies alongside data analysis. Several factors contribute to a city's position in the global index of smart cities, such as technological infrastructure, sustainability measures, and citizen participation.

The technological infrastructure of a city forms the backbone of its smart initiatives. This includes high-speed internet connectivity, widespread deployment of sensors, and integration of various systems into a centralized platform. With a strong technological base, cities can efficiently collect and analyze data, allowing them to make informed decisions and provide efficient services.

In addition, smart cities prioritize cybersecurity to protect their networks from potential threats. With increasing dependence on technology, ensuring the security of data and systems is crucial for maintaining public trust and avoiding disruptions.

Another important aspect of smart cities is their commitment to sustainability. By adopting eco-friendly practices and harnessing renewable energy sources, cities can reduce their carbon footprint and contribute to a greener future. This includes initiatives such as smart grid systems, energy-efficient buildings, and waste management solutions.

To promote sustainable mobility, smart cities often invest in advanced transportation systems, such as infrastructure for electric vehicles and intelligent traffic management. By reducing congestion and emissions, these cities strive to create a more sustainable and viable environment for their residents.

Moreover, the success of a smart city largely depends on the active participation and engagement of its citizens. By providing platforms for open communication and collaboration, cities can foster a sense of belonging and involvement among residents. This can be achieved through digital applications, community forums, and active information programs that encourage civic participation.

Additionally, smart cities prioritize inclusivity and accessibility to ensure that the benefits of technology are accessible to all members of the community. This involves bridging the digital divide and implementing measures that respond to the needs of diverse populations.

7. Lessons identified regarding quality critical infrastructure

Leaders of the G20 have emphasized the importance of investing in quality infrastructure at the Hangzhou Summit to deliver high-quality infrastructure projects, where quality infrastructure investment is defined as: *"aiming to ensure economic efficiency, taking into account life-cycle costs, safety, resilience against natural disasters, job creation, capacity building, and the transfer of expertise and know-how on mutually agreed terms and conditions, while addressing social and environmental impacts and aligning with economic and development strategies"*.

Firstly, economic efficiency considers the triple constraint, traditionally consisting of only time, cost, and scope. These are the primary constraints of competing projects that we must be most aware of when it comes to critical infrastructures and the resources that lead to project completion. The triple constraint is illustrated in the form of a triangle to visualize project activity and to see the relationship between scope/quality, schedule/time, and cost/resource.

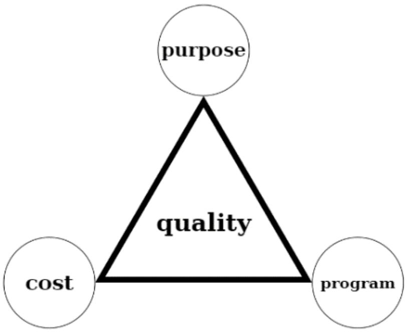


Figure no. 4. Diagram of the triple constraint triangle

Sustainability and longevity of infrastructure assets are essential as they simultaneously address the needs and meet the expectations of end users, and the relationship between decisions made during design and construction and how they aim to minimize costs over the entire asset lifecycle is important as it leads to meeting the requirements of end users.

Therefore, lessons identified regarding quality critical infrastructure include the importance of proper planning and design, the use of sustainable materials and techniques, as well as the implementation of strict policies and regulations to ensure high-quality standards. Additionally, it is essential to pay attention to regular maintenance and repairs to keep the infrastructure in good condition.

Conclusions

In conclusion, critical infrastructure plays a crucial role in the development of smart cities and in enhancing the quality of life for residents. Well-developed and managed critical infrastructure ensures a safe and secure environment, as it includes communication systems, electricity and water networks, as well as transportation and healthcare infrastructure.

Sustainable and resilient infrastructure is vital to address climate change and other natural threats. Investments in green technologies, as well as in the construction and renovation of energy-efficient buildings, can significantly contribute to protecting the environment and reducing the impact on natural resources.

The quality of life through infrastructure is essential for the well-being and prosperity of communities. Investments in critical infrastructure can have a significant impact on how people live and work in a particular urban or rural environment.

Strategic planning and efficient governance are essential to ensure high-quality infrastructure. This involves engaging stakeholders and the community in the decision-making process, as well as adopting appropriate policies and regulations for the efficient management and maintenance of infrastructure.

By building well-developed critical infrastructure, connectivity and accessibility in cities are facilitated. This is achieved through digital critical infrastructure, such as internet networks and communication services, which enable easier and faster communication and access to information.

All of these contribute to improving the quality of life by providing better and more efficient services.

Therefore, investments in critical infrastructure are essential so as to improve the quality of life and to create sustainable and resilient environments in communities. By addressing these aspects in an integrated and strategic manner, infrastructure can contribute to meeting the current and future needs of society.

BIBLIOGRAPHY:

1. Alexander, Soley. 2021. “Quality of Life Through Infrastructure”. 2021. Accessed January 6, 2024. https://www.rtinsights.com/quality-of-life-through-infrastructure/. (In-text citation: Alexander Soley 2021).
2. Alicia, Bárcena *et. al*. 2021. “Desastres y desigualdad en una crisis prolongada”. 2021. Accessed January 7, 2024 https://www.cepal.org/es/publicaciones/47375-desastres-desigualdad-crisis-prolongada-sistemas-proteccion-social-universales. (In-text citation: Alicia Bárcena *et. al* 2021)
3. Clemens, Sanetra; Rocío, M. Marbán. 2020. “Enfrentando el Desafío Clobal de la Ciudad: una Infraestructura Nacional de la Ciudad”. 2020. Accessed December 19, 2023. https://www.google.ro/books/edition/Enfrentando_el_Desafio_Clobal_de_la_Ciud/VG0TqezOh2gC?hl=ro&gbpv=1&dq=infraestructura+e+calidad+de+vida&pg=PA3&printsec=frontcover. (In-text citation: Clemens Sanetra and Rocío M. Marbán 2020).
4. Daniel, Taras. 2019.” Infraestructura sostenible e infraestructura de calidad:

dos caras de la misma moneda". 2019 Accessed December 15, 2023. https://blogs.iadb.org/sostenibilidad/es/sustainable-infrastructure-and-quality-infrastructure-are-two-sides-of-the-same-coin/. (In-text citation: Daniel, Taras. 2019).

5. Gareis, Philipp *et al.* 2021. "Infrastruktur als Aspekt von Lebensqualität und ihr Einfluss auf die Lebenszufriedenheit von Bewohnern in Kleinstädten des Regionstyps zentrale Lage in Deutschland". 2021. Accessed 16, 2023. https://www.econstor.eu/handle/10419/232566. (In-text citation: Gareis, Philipp *et al.* 2021).
6. Gizem,Yalcin; Stefano, Puntoni. 2023. "How AI Affects Our Sense of Self". 2023, Accessed 20, 2024. https://hbr.org/2023/09/how-ai-affects-our-sense-of-self. (In-text citation: Gizem Yalcin and Stefano, Puntoni 2023).
7. Inés, Sánchez de Madariag. 2004. "Infrastructuras para la vida cotidiana y calidad de vida". 2004. Accessed December 15, 2023. https://www.researchgate.net/publication/28219632_Infraestructuras_para_la_vida_cotidiana_y_calidad_de_vida. (In-text citation: Inés Sánchez de Madariag 2004).
8. Jayna, Locke. 2023. "Las 10 ciudades inteligentes más futuristas del mundo". 2023. Accessed January 20. 2024. https://es.digi.com/blog/post/smart-cities-in-the-world.
(In-text citation: Jayna Locke 2023).
9. Manuel, Sánchez, Gómez-Merelo. 2018. "La seguridad y las infraestructuras críticas". 2018. (In-text citation: Manuel Sánchez Gómez-Merelo 2018, 14).
10. Naturklima. 2022. "Informe de Impacto y Vulnerabilidad al Cambio Climático en Gipuzkoa". 2022. (In-text citation: (Naturklima 2022).
11. Romanian Intelligence Service. "Critical Infrastructure Protection". Romanian Intelligence Service, Critical Infrastructure Protection, 5).
12. Tsuyoshi, Takano *et al.* 2023. "Evaluating the quality of life for sustainable urban development". 2023. Accessed December 15. 2023. https://www.sciencedirect.com/science/article/pii/S0264275123003736. (In-text citation: Tsuyoshi Takano et al. 2023).
13. Yoshitsugu, Hayashi et al.2023. "Quality of Life Assessment in Urban Development and Transport Policymaking". 2024. Accessed December 16. 2023.
https://www.adb.org/publications/quality-of-life-assessment-in-urban-development-and-transport-policymaking. (In-text citation: Yoshitsugu, Hayashi et al. 2023).
14. https://op.europa.eu/webpub/eca/special-reports/electrical-recharging-5-2021/en/.
Accessed January 6. 2024.
15. https://s2grupo.es/la-seguridad-en-infraestructuras-criticas/. Accessed January 7. 2024.
16. https://www.target-tecnologia.es/blog/target-institucional/la-seguridad-en-las-infraestructuras-criticas/. Accessed January 7. 2024.
17. https://blogs.iadb.org/ciudades-sostenibles/es/como-puede-la-infraestructura-sostenible-mejorar-la-calidad-de-vida-y-la-inclusion-social-en-america-latina/. Accessed January 10. 2024.
18. https://nexusintegra.io/es/infraestructuras-inteligentes-la-clave-para-las-ciudades-inteligentes/. Accessed January 20. 2024.
19. https://www.tomorrow.bio/es/post/las-principales-ciudades-inteligentes-del-mundo-en-2023-2023-08-4907009781-iot. Accessed January 20. 2024.
20. https://www.jll.es/es/analisis-y-tendencias/ciudades/que-retos-debe-superar-una-ciudad-para-ser-sostenible. Accessed January 20. 2024.
21. https://opentextbc.ca/projectmanagement/chapter/chapter-2-what-is-a-project-project-management/. Accessed 22. 2024.
22. https://www.ppiaf.org/documents/5819. Accessed January 27. 2024.

1053477-3045-1396-24-41

CYBERSECURITY WITHIN CRITICAL INFRASTRUCTURES

Sabina-Trandafira ROȘCA
Sg., Command and Staff Faculty,
"Carol I" National Defense University, Bucharest, Romania

***Abstract**: Cybersecurity in critical infrastructures is a major concern in the contemporary world. As people are increasingly dependent on technology and digitally interconnected, cybersecurity has become a vital element in protecting critical infrastructures. This interdependence brings risks and threats to the fundamental systems that support the functioning of modern society. Governments, organizations, and society as a whole must protect critical infrastructure against cyber threats by implementing advanced technical cybersecurity measures, creating integrated policies and strategies, fostering collaboration between the public and private sectors, and continuously investing in research and development to anticipate and counter emerging threats in the cybersecurity domain.*

Keywords: *Cybersecurity; critical infrastructures; evolution; cyberattacks; cyber threats*

Introduction

Over time, from year to year, cyber threats have evolved in complexity, forms of manifestation and frequency, as a result of advances and innovations in the field of IT&C, as well as the large-scale introduction of technologies that facilitate online interaction. While at the beginning of the 90s, cyber security was an exclusive issue for the IT departments of public and private institutions, nowadays, due to the quantitative and qualitative growth of cyber threats, the specific concerns related to the domain have moved to the strategic level of these departments. Therefore, we can talk about a radical change in the field, which includes changing the essential terms that describe cyber security.

Critical infrastructures are the backbone of modern society, supporting the efficient functioning of various sectors and daily life. From the source of electricity that powers our homes and businesses, to the transport networks that facilitate the flow of goods and people, to the financial and communications systems that support economic and social activity, these infrastructures are a vital part of modern life.

An increasingly pronounced trend in recent decades has been to digitize and interconnect these critical infrastructures to make them more efficient and easier to manage. However, this increased reliance on information and communication technologies brings with it significant cybersecurity risks. Attacks on these critical infrastructures have become increasingly common, with the potential to disrupt the functioning of society and cause significant economic damage.

This evolution of critical infrastructures to the digital environment brings considerable benefits, but also increases their vulnerabilities to cyber threats. Intrusions into industrial control systems, compromise of power grids, and attacks on financial systems are just a few examples of the risks critical infrastructure faces in the digital age.

Cybersecurity and critical infrastructures

There are certain types of infrastructure that are essential to our economy, safety and lifestyle. These complex, often interconnected systems, have become so common and essential to our daily activities. When the services provided by this infrastructure are interrupted, such as the loss of access to electricity, medical services, telecommunications, transport or water, we become aware of their importance. To assess the vulnerability of these infrastructures, it is essential to understand and define the relevant terminology (Robin 2017).

Although the terminology and definitions of "critical infrastructure" may vary from country to country, there are a number of common and fundamental elements.

In Australia, critical infrastructures are physical resources, sources of supply, information technology and communications networks that, if destroyed, damaged or inaccessible for a long period of time, could have a significant impact on the social or economic well-being of the country or would affect Australia's ability to protect and ensure its national security.

In Germany, "critical infrastructures are organizations and resources of particular importance to a community whose failure or insufficiency would cause a sustained shortage of goods, significant disruptions to public order or other dramatic consequences".

In the American Heritage Dictionary, "infrastructure" refers to the basic amenities, services, and facilities that are necessary for the functioning of a community or society, such as water and power networks, transportation and communication systems, and public institutions such as schools, post offices and prisons. This definition and others like it are, however, broad and subject to interpretation. In practical terms, what is considered infrastructure depends largely on the context in which the term is used.

Within US public policy, the conceptualization of the term "infrastructure" has undergone a certain evolution and has often been characterized by ambiguity. Two decades ago, "infrastructure" was predominantly defined in the context of debates on the adequacy of national public works, considered by many to be in a state of deterioration, obsolescence and insufficient capacity. At the time, the Council of State Planning Agencies defined "infrastructure" as "a diverse array of public facilities and equipment essential to the provision of social services and support to private sector businesses," according to a representative report. This report indicated that infrastructure included such items as roads, bridges, water and sewage systems, airports, ports, and public buildings. It could also include schools, medical facilities, prisons, recreation areas, power generation facilities, fire safety measures, waste management and communications services (Vaughan 1984).

As a result of PCCIP's efforts, the term infrastructure, which is defined as "the foundation or basic framework (as a system or organization)", has gained meaning and relevance. In a report the Commission sent to the US President in October 1997, it defined infrastructure as a network of independent systems and processes, mostly privately owned, that are created by people and that work together to produce and distribute vital goods and services in a continuous flow.

The Critical Infrastructure Assurance Office (CIAO), which was established under Executive Order 63 to help coordinate the federal government's critical infrastructure protection initiatives, later expanded and refined this definition. Infrastructure, as defined by the CIAO, is the set of interdependent networks and systems that include industries, institutions, people, procedures, and distribution capabilities that ensure the safe flow of products and services that are essential to the defense and economic security of the United States and to the proper functioning of the government.

According to EC Directive 114/2008; OU 98/2010, critical infrastructure is defined as an element, system or component thereof that is essential for maintaining the vital functions of society, such as health, safety, security, social or economic well-being of people. If it were to be disrupted or destroyed, it would have a significant effect at the national level, as it would not be able to retain those functions.

National Critical Infrastructure (NCI) is an element, system or component that is located on the national territory and is essential for maintaining important functions of society, such as health, safety, security, social or economic well-being of people. If it were to be disrupted or destroyed, it would have significant national influence as a result of its inability to maintain these functions.

European Critical Infrastructure (ICE) is a national critical infrastructure, the disruption or destruction of which would have a significant impact on at least two member states of the European Union. The impact is assessed using cross-sectoral criteria. This includes the effects associated with intersectoral dependency relationships with other types of infrastructure.

The main characteristics of critical infrastructures

Interdependence is the first characteristic that shows how strong the links between systems are, which means that one sector (and this also applies to sub-sectors) is not operational without the other sector, as demonstrated by the following ideas: "Some sectors of critical infrastructure are mainly dependent on electricity and telecommunications systems, as well as cyber risks." It can be said, without exaggeration, that the repercussions of electricity interruptions affect all sectors" (Miklós 2021). The interdependence of critical infrastructures can be grouped physically, information technologically (cyber), geographically and logically (Rinaldi 2001). Thus, physical dependence occurs when the normal operation of the sector requires the intervention of another sector. Dependence on IT occurs when the sector is managed by information technology. There is geographic dependency when sectorial elements are installed in geographical proximity to each other and thus interact in the event of a failure. Logical dependency refers primarily to the human factor (Horváth 2016).

The next characteristic is the network, which means interconnected critical infrastructures, a complex system whose sectoral elements continuously interact with each other. Interdependence and networking can be directly deduced from the domino principle, or domino effect, as a characteristic of critical infrastructures. This means that damage to one critical infrastructure sector can impact the functioning of several sectors, which together can have a strong social, economic and therefore political impact. One of the main examples of this is the 2003 blackouts in Italy and Switzerland, and those in Austria, Slovenia and France. Between 50 million and 60 million people lost electricity as a result of these events (Miklós 2021).

Scaling and location are very important characteristics of critical infrastructures. An inadequate positioning can lead to terrible situations, as evidenced by the installation of diesel-powered safety generators to cool the Fukushima reactors in flood-free areas, which contributed significantly to the disaster. We can also take as an example the location of CERN, whose accelerator LHC (Large Hadron Collider) is very close to Geneva airport (Miklós 2021). Information systems, as the main characteristic of critical infrastructures, show that all sectors operate almost completely automated using IT systems (Miklós 2021).

All necessary safeguards should therefore be taken to ensure that no sector is attacked within the territory of a Member State.

Cybersecurity is the art of preventing unauthorized access or illegal use of networks, devices and data. In addition, it refers to annual practices that ensure that data is private. Nowadays, it seems that everything depends on computers and the Internet. This applies to all domains, including communication (e.g. email, tablets, smartphones), entertainment (e.g. social apps, video games), transportation (e.g. navigation systems), shopping (e.g. credit cards, online shopping), medical services (e.g. medical records, medical equipment).

As a result of the analysis of the specialized literature, we selected 3 definitions of cyber security:

- "Cyber security uses defensive methods to detect potential intruders" (Kemmerer 2003).

- “Cybersecurity is about reducing the likelihood that a malicious attack will affect software, computers and networks. This includes tools that are used to detect intrusions, stop viruses, block malicious access, require authentication, enable encrypted communications, and more” (Amoroso 2006).
- “Cybersecurity means all security tools, rules, ideas, safeguards and concepts, as well as risk management methods, actions, training, assurance measures and technology that can be used to protect the cyber environment and assets of the organization and users” (ITU 2009).

An analysis of the three definitions of cybersecurity provided by Kemmerer, Amoroso, and UIT reveals a complex and ever-evolving perspective on the concept of cybersecurity. Each definition emphasizes distinct aspects of this field highlighting the diversity of approaches and strategies needed to protect the digital environment.

The definition proposed by Kemmerer emphasizes the defensive methods used to detect potential intruders. This perspective reaffirms the importance of detecting and countering threats to the security of information systems, emphasizing the need for continuous surveillance and rapid reaction to possible attacks. In contrast, Amoroso's definition expands the concept of cyber security to include a wider range of tools and techniques used to prevent and detect cyberattacks and on the other hand, the definition provided by the ITU expands the concept of cyber security to include not only the technical aspects, but also the practical and strategic aspects of protecting the cyber environment and the assets of the organization and users.

Together, these definitions outline a complex cybersecurity landscape, highlighting the need for a multidimensional approach and constant adaptation to evolving threats and technologies.

Historic evolution of cyber threats

Over time, cyber threats have evolved in complexity as a result of advances and innovations in IT&C and the widespread introduction of technologies that facilitate online interaction. Contrary to popular belief, cyber security concerns are not a phenomenon of the 1990s. Computer viruses have been part of the background noise of cyberspace even from an early period. In his analysis of cyber aggressions, Dumitru Dumbravă exemplifies this type of threat through an example from the movie "War Games", produced in 1986, in which a young teenage hacker manages to, by means of his personal computer, command and control the American nuclear arsenal (ITU 2009). In addition, the famous "Cuckoo's Egg" incident of the 1980s drew attention to the fact that spy organizations had discovered new methods of collecting classified information through computer networks. In this context, debates on cyber themes originated in the United States in the mid-90s, from where they later spread to other developed countries and are placed in a variety of forms on the agenda of security policies (ITU 2009).

In 1988, Robert Morris, a young graduate of Cornell University in the USA, developed the first virus that infected about 6000 systems, which at that time represented about 10% of all computers connected to the Internet. This was the first notable cyberattack. Named the Morris Worm, it was the first malware to successfully execute a Denial-of-Service (DoS) attack. Administrators of regional Internet networks have taken the decision to disconnect them to eliminate the infection. This was done within a few days. As a result, the global internet network was disrupted for several days (Rog 2024).

Since the 2000s, the complexity of cyber threats has begun to increase, and Trojan-type applications have taken the first steps toward anonymizing the attackers' true purpose. Since cyberespionage activities were initiated on a large scale in the first decade of the 21st century, they have been used by both cybercriminal actors and strategically motivated entities. In this regard, the APT1 and APT28 groups targeted assets in the governmental (foreign affairs, military public administration) and private (financial, aerospace, IT&C, transport) domains (Rog 2024).

As for NATO, the Alliance's cyber security was first addressed at the strategic level at the 2002 Prague Summit. Allied nations felt that it was necessary to protect the computer systems that were supposed to be used at the Riga Summit in 2006. The years 2007-2008 were crucial for the current definition of the cyber security environment, as it was the first time that an organization strategically motivated a cyberattack on the IT&C infrastructure of other states. At the same time, this can be considered the moment when "cyber weapons" began to be used on a large scale. In January 2008, NATO adopted the first Alliance Strategy on Cyber Defense (Rog 2024).

In terms of cyber threats, 2010 marked a significant change. As a result, a new form of threat manifestation was revealed, known as cyber sabotage, which refers to the Stuxnet worm application, which aims to cause significant material damage. Technologically, Stuxnet was designed to exploit zero-day vulnerabilities to compromise the equipment that managed the centrifuges used to produce and enrich uranium (Rog 2024).

In 2013, the adoption of Government Decision no. 271/2013, which approved Romania's Cyber Security Strategy, was another significant moment for cyber security. The decision of the Supreme Council of National Defense designated the SRI as the national authority in cyberintelligence (Rog 2024).

In 2016, at the Warsaw Summit, NATO heads of state and government determined that cyberspace should be an operational domain alongside land, air and water. This aspect helped NATO meet its objectives of defending Allied cyberspace (Rog 2024).

In 2017, the EU institutions took an important step towards strengthening their cooperation in combating cyber-attacks. For all EU institutions, bodies and agencies, an inter-institutional agreement that entered into force in 2017 establishes a Cyber Security Incident Response Center (CERT-EU). This enhanced the existing operations group, turning it into a stable and effective team tasked with ensuring a coordinated EU response to cyberattacks against its institutions. CERT-EU works closely with the internal cybersecurity teams of the EU institutions and communicates with the Cybersecurity Incident Response Centers and IT security companies in the Member States and other countries, exchanging information on threats and methods of managing them. In addition, the center works closely with its NATO counterparts.

In 2018, Member States' ambassadors approved the Cybersecurity Act, which turned the European Network and Information Security Agency (ENISA) into a permanent EU cybersecurity agency. Since its establishment in 2004, the Greece-based agency ENISA has helped protect EU networks and information. Thus, during the respective year, ENISA received tasks to support member states, EU institutions and other interested parties in cyber matters. It would support the EU policy on cybersecurity certification, for example by taking a major part in the preparation of certification systems and encourage the adoption of new certification systems, for example by creating a website providing information on certificates. The agency would also organize regular EU-wide cyber security exercises, including a large-scale comprehensive exercise every two years.

In 2019, the Council established a framework that allows the EU to implement specific restrictive measures to prevent and respond to cyberattacks that pose an external threat to the EU or its Member States. These restrictive measures are considered necessary to achieve the objectives of the common foreign and security policy (CFSP). The EU can sanction individuals or organizations that conduct cyberattacks or attempted cyberattacks, as well as those that provide financial, technical or material support to such attacks. Penalties may be imposed on individuals or organizations related to them. The restrictive measures include freezing the assets of individuals and organizations as well as denying access to people traveling to the European Union. In addition, EU individuals and entities are prohibited from providing financial assistance to individuals on the list.

Cybercrime affects different economic sectors in different ways, as a 2020 study shows: it was the most disruptive fraud phenomenon in government and public administration, technology, media and telecommunications and in the health sector. It also ranked second among the most disruptive fraud phenomena in the financial, industrial and manufacturing sectors.

The EU Council adopted a new directive in 2022: NIS 2, which is an update of the previous directive from 2016. The main objective of the directive is to improve cyber security in the European Union (EU). NIS 2 also sets out a number of new cyber security measures to be implemented by regulated entities. These measures include implementing a cyber risk management program, implementing appropriate technical and organizational measures to address identified cyber risks, reporting cyber security incidents to the relevant authorities.

Examples of cyberattacks on critical infrastructures

In 2013, Iranian hackers allegedly gained access to America's Bowman Avenue Dam, located about 30 kilometers from New York. Investigators believe the hackers were only trying to test their skills in the attack on New York's dam computers because they were unable to gain operational control of the locks.

In Ukraine, between July 2014 and July 2018, several critical infrastructures (energy supply, transport sector, drinking water supply, banking system and financial markets) were attacked by Russian hacker groups. In July 2014, Russian hacker groups CyberBerkut and GreenDragon gained unauthorized access to PrivatBank's system and disclosed confidential information (account details, phone numbers, etc.). On December 23, 2015, after several months of work, the APT 28 group launched a remote attack, disrupting electricity supply services to customers in Kyiv, Prykarpattia and Chernivtsi. The attack left about 225,000 consumers without power and heating for six hours. This was the first publicly documented cyberattack against a power grid control system (Whitehead 2017).

Also, a malware called BlackEnergy was detected in time, a month later, in the network of Borispil International Airport near Kiev, so that the hackers could not carry out the cyberattack. Researchers say the previous attacks may have overlapped with smaller attempts between November and December 2015 targeting Ukrainian mining and railway systems (with malware such as KillDisk and BlackEnergy) (Miklós 2021). In 2017, a ransomware virus called NotPetya (which initially targeted Ukraine but reached business circles around the world) affected several sectors, including critical infrastructure sectors. The cyberattacks targeted the Ukrainian government, the energy sector (Chernobyl radiation monitoring station), the banking sector (National Bank of Ukraine and nationwide ATMs), and the transport sector (the electronic payment system in the Kyiv metro). In July 2018, the Security Service of Ukraine succeeded in combating a sabotage operation targeting the drinking water supply. Due to the prominent role of the infrastructure, if the attack had been successful, it would have caused severe water supply problems nationwide (Marazis 2018).

In 2019, a number of ransomware attacks against businesses operating in Germany were identified. Called Germanwiper, this ransomware can replace infected files with zeros and ones, making their recovery impossible. The ransomware is spread through email phishing campaigns and has particularly targeted HR staff at leading enterprises by being embedded in fake job applications.

The crucial importance of protecting critical infrastructures is also underlined by the cyber incident at a hospital in Düsseldorf in December 2020, which had fatal consequences - a first such case in Europe. The hospital in Düsseldorf, Germany, was primarily affected by a cyberattack that crippled emergency management software, according to the Associated Press. Thus, several patients who had come to the Emergency Reception Unit were redirected to other hospitals and a woman died because she did not receive medical care in time. A nearby university, not the hospital, was the target of the cyberattack, according to the first information provided by German authorities.

Cyberattacks on critical infrastructure by state actors - detected by Microsoft - increased from 20% to 40% in 2022. This increase was the main result of Russia's intention to damage Ukraine's infrastructure and aggressively spy on Ukraine's allies, including the United States. In addition, Russia has increased its efforts to compromise IT companies, attempting to disrupt or collect information from government agencies in NATO member countries that are customers of these companies. 90% of Russian and Microsoft-identified attacks in the past year targeted NATO member states, and 48% targeted IT companies based in NATO countries (Burt 2022).

Also in 2022, China stepped up cyberattacks for espionage and information theft in an attempt to increase its influence in the Southeast Asian region and thus thwart the growing interest of the United States. In February and March, a Chinese state actor carried out an attack that targeted 100 accounts affiliated with an intergovernmental organization in Southeast Asia, even as the organization announced a meeting between the U.S. government and regional leaders. Microsoft discovered malware from a Chinese state actor in Solomon Islands government systems shortly after the countries (China and Solomon Islands) signed a military agreement. China used its cyber skills to attack Southern Hemisphere nations such as Namibia, Mauritius, Trinidad and Tobago.

A recent CERT-UA report revealed that Sandworm attackers caused disruptions to communications systems on the IT networks of 11 telecommunications service providers in Ukraine from May to September 2023. Sandworm is a criminal cyber-espionage group linked to the GRU, and Russian attackers orchestrated attacks in 2023 using phishing lures, Android malware and data-wipers.

The main types of cyberattacks

Malware, or "malicious software," such as viruses, worms, trojans, spyware, and ransomware, is the most common type of cyberattack. Malware infiltrates systems by asking users to click on a link to a suspicious website, via email by downloading an infected attachment, or by downloading unwanted software. The respective malware, once installed, has the ability to track the user's activities, send confidential information to the attacker, help the attacker penetrate other targets on the network, and even cause the user's device to be connected to a botnet (a network that includes a number of devices connected to the Internet) used by the attacker for malicious purposes. The attacker also has the ability to destroy data or shut down the system completely.

Worms are programs that can self-replicate by transmitting their own copies on the network, which causes damage by loading the tape.

Trojans are programs designed to steal confidential data or allow access to the system to unauthorized users. Regarding mobile terminals, the F-Secure company report from 2012 states that 84% of threats are represented by Trojans, with the aim of obtaining financial gains.

Drive-by threats have the ability to automatically exploit vulnerabilities in software installed on a computer without having to contact the legitimate user. When users visit sites that contain drive-by exploits, vulnerabilities in browsers, plugins, or operating systems can be exploited to install malware on their computers without their knowledge.

APT is a cyberattack with a high degree of complexity, launched by motivated groups to constantly attack a target in order to obtain confidential data, being specific to cyber espionage companies.

Phishing is a type of online deception that uses methods to manipulate the identity of individuals or organizations in order to obtain material benefits or confidential information. Attackers force their victims to reveal identifying information by using various social engineering techniques. The most common targets are the locations of financial institutions such as banks, online payment services, social networks, Internet service providers, non-profit organizations, or the websites of certain government sectors are other targets of this type of cyberattack.

Ransomware is a type of malware that demands an amount of money from the victim, threatening to publish, delete or keep important personal data. Among them, we could mention:

- Crypto Ransomware: This type of ransomware spreads through computers or networks especially looking for important information. It collects documents such as text, images, spreadsheets and PDFs to encrypt them. You will usually be able to continue using your computer and the rest of your data will not be affected. However, the encrypted data will be inaccessible, and the malware will try to force you to pay a ransom to unlock it. Most types of ransomware demand victims between $200 and $900. The date is usually deleted forever if the ransom is not paid within 48-72 hours (Porter 2024).
- Locker Ransomware: It restricts all access to your computer and data.
- Scanner: A system that scans entire groups of IPs on the Internet, in order to identify vulnerable systems, on which the cyberattack will be launched later.
- Sniffer: A system that intercepts data packets transmitted through networks, which it later decodes, in order to find out passwords or confidential data.
- Open Proxy: non-secure server that can be used by any Internet user, in order to launch attacks against various targets, which allows him to keep his identity hidden.

A botnet is a group of computers that an attacker controls. These faulty systems are called "robots" or "zombies". This is a network of infected computers that are not controlled by their owners. A botnet can be used for a variety of reasons: Denial of Service - DDoS attacks, spamming, identity theft, malware distribution, infecting computer systems, and more (Neagoe 2016).

Security threats evolve as attackers become more professional. If cyberattacks in the past were launched by disgruntled hackers in order to gain recognition, nowadays, attacks are launched by professionals, through complex methods, in order to obtain confidential data and financial gains.

Conclusions

In an increasingly digitally interconnected world, the cyber security of critical infrastructures cannot be neglected. Only through a holistic approach and sustained efforts can we ensure that critical infrastructures remain resilient in the face of cyber threats and continue to support the efficient functioning of modern society.

Additionally, as technologies evolve and infrastructures become more interconnected, the attack surface for potential cyber attackers increases significantly. For example, the integration of the Internet of Things (IoT) into various aspects of critical infrastructure, such as monitoring and control systems, opens up new attack vectors and increases exposure to security risks.

It is also important to emphasize that cybersecurity of critical infrastructures is not only a technical issue, but also a strategic and geopolitical one. Cyber attacks on critical infrastructures can have serious national and international security consequences, leading to major economic disruptions, political destabilization and even threats to the lives and safety of citizens.

Therefore, protecting critical infrastructures against cyber threats is a crucial priority for governments, organizations and society as a whole. This involves not only the implementation of advanced technical cybersecurity measures, but also the development of integrated policies and strategies, collaboration between the public and private sectors, and continuous investment in research and development to anticipate and counter emerging cybersecurity threats.

BIBLIOGRAPHY:

1. Visarion Neagoe, Silviu-Stelian Borșa, *Riscuri și amenințări cibernetice la adresa securității internaționale. Terorismul cibernetic – un flagel care amenință securitatea cibernetică*, Revista de Științe Militare, 4/2016
2. David E. Whitehead, Kevin Owens, Dennis Gammel, Jess Smith, „*Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies”*, in Power and Energy Automation Conference, Spokane, Washington, 2017
3. Miklós Böröcz. *"Politicile Privind Protecția Infrastructurilor Critice La Nivel European"*, Impact strategic nr 3, 2021.
4. Andreas Marazis, Rober Kothe, „Russian Cyberwarfare Capabilities: *Assessing the Threat for Ukraine's Critical Infrastructure”*, in European Neighbourhood Council Analysis, 2018
5. Cosma Robin, *Considerații privind managementul situațiilor de urgență din perspectiva asigurării*, București, 2017
6. S. M. Rinaldi, J. P. Peerenboom and T. K. Kelly, „*Identifying, understanding, and analyzing critical infrastructure interdependencies*”, in IEEE Control Systems Magazine, vol. 21, nr. 6, 2001
7. Attila Horváth, „*Noi riscuri privind infrastructurile critice și dezvoltarea tehnologică, partea a doua*”, in Hadtudomány, 2016
8. Olguţa Dogaru, *"Noi provocări în securitatea cibernetică",* Studii de securitate publică 4:118-122
9. Strategia Națională pentru protecția infrastructurilor critice , Germania, 2009
10. The American Heritage Dictionary of the English Language, Fourth Edition. Houghton, January 2006
11. Merriam Webster's Collegiate Dictionary (10th ed.), Springfield, MA, 1993.
12. ITU, *Overview of Cybersecurity.Recommendation ITU*, Geneva: International Telecommunication Union, 2009
13. Vaughan, R. and Pollard, R. Rebuilding America, Vol. I, *Planning and Managing Public Works in the 1980s*. Council of State Planning Agencies. Washington, DC. 1984. pp 1-2.
14. Kemmerer, R. A, 2003, *Cybersecurity*, Proceedings of the 25th IEEE International Conference on Software Engineering: 705-715.
15. Amoroso, E. 2006, *Cyber Security*, New Jersey: Silicon Press
16. Dumitru Dumbrava, *Agresiunile în spaţiul cibernetic*, Revista Română de Studii de Intelligence nr. 6 / decembrie 2011
17. Anton Rog şi Cristian Condruţ, *Evoluția amenințării cibernetice,* https://intelligence.sri.ro/evolutia-amenintarii-cibernetice, accesed 31 January 2024
18. 2 PWC, Fighting fraud: A never-ending battle, PwC's Global Economic Crime and Fraud Survey, 2020.
19. Directiva CE 114/2008; OU 98/2010
20. Liniile Directoare naționale pentru protejarea infrastructurii critice împotriva terorismului ale Guvernului Australian

21. Presidential Decision Directive 63, Available: http://www. ciao.gov
22. Evan Porter, *Ce este Ransomware*, https://ro.safetydetectives.com, accessed 31 January 2024
23. Raport Microsoft Digital Defense 2022, https://news.microsoft.com, accessed 31 January 2024
24. www.cert.ro, accessed 31 January 2024
25. Tom Burt – Corporate Vice President, *Customer Security & Trust*, https://news.microsoft.com, 2022, accessed 31 January 2024
26. www.consilium.europa.eu, accessed 31 January 2024
27. www.sri.ro, accessed 31 January 2024
28. America's Cyber Defense Agency. [Online]. Available: https://www.cisa.gov, accessed 6 December 2023
29. Cybersecurity Insiders, GermanWiper Ransomware attack warning for Germany, www.cybersecurity-insiders.com, accessed 31 January 2024

1053477-3045-1396-24-42

IOT AND CRITICAL INFRASTRUCTURES: TECHNOLOGICAL TRANSFORMATION AND SECURITY IMPLICATIONS

Eliza-Mihaela CĂLIN
Slt., Bucharest, Romania
E-mail: elizacalin277@gmail.com

Abstract: The *Internet of Things (IoT) is a concept that defines the communication and relationship between different types of devices through the Internet (Barbu, 2023). Specifically, the Internet of Things is a network through which data and information are transferred between different devices without human intervention (Coursera, 2023). Previous analysis reveals that the increasing use of IoT devices in critical infrastructures has brought significant benefits in terms of efficiency and monitoring, but has exposed systems to increased security risks such as cyber-attacks, software vulnerabilities, or unauthorized access. However, a clear understanding of how to manage these risks has not been developed.*

This paper explores the growing impact of the Internet of Things on critical infrastructures and reveals significant security concerns. Critical infrastructures, such as energy or transportation systems, are becoming increasingly dependent on IoT technology, raising concerns about their vulnerability to cyber threats.

The central research question addressed in this article is "What are the implications of the growth of IoT on the security of critical infrastructures and how can they be effectively managed to ensure adequate protection against cyber threats?".

To answer the research question, this article is based on an interdisciplinary approach that combines theoretical analysis with concrete case studies from various critical infrastructure sectors. It will therefore analyze existing security models and propose technical solutions and risk management strategies.

The results highlight the importance of prioritizing cybersecurity within critical infrastructures affected by IoT and propose solutions to effectively address identified vulnerabilities. In order to ensure the continuous and secure operation of critical systems in the IoT era, the need for proactive collaboration between cybersecurity and critical infrastructure stakeholders will be highlighted.

Keywords: *internet of things, security, critical infrastructures*

Introduction

The "Internet of Things" is a recently developed technology that refers to the interconnection of various appliances, devices, and computers via the Internet.

IoT technology is used in a variety of applications including healthcare, industries, educational institutions, power plants, and homes to interconnect machines and appliances and control them remotely over the internet. IoT uses the four-layer model for communication, so different protocols and technologies are used at different layers. IoT can use wireless sensors, radio frequency IDs, Wi-Fi, or Bluetooth modules. Given the diversity of connected devices in IoT, the cloud is used to store their data. The use of data clouds, a large number of interconnected devices, and Wi-Fi technology have made IoT vulnerable to multiple security attacks (Khan, *et al.*, 2023).

Content

IoT is an indispensable tool today for the use of critical infrastructures, enabling their effective monitoring and management. Sensors and automation optimize the operations needed to manage critical infrastructures. However, the expansion of IoT also brings cybersecurity risks, making threat protection essential for the safe and reliable operation of these systems.

To date, there has been a notable gap in the literature regarding the specific impact of IoT technology on critical infrastructures and their security. Most studies have focused on either IoT or critical infrastructures, but few have analyzed in detail the interaction between the two and the security implications. Previous studies have found that the increased use of IoT devices in critical infrastructures has brought significant benefits in terms of efficiency and monitoring, but has also exposed systems to increased security risks. These risks include cyber-attacks, software vulnerabilities, and unauthorized access.

The article examines the impact of the growth of the Internet of Things on critical infrastructures and their security. Critical infrastructures, for example, energy or transport networks, are becoming increasingly dependent on IoT technologies, raising questions about their vulnerability to cyber threats.

This article also provides an in-depth analysis of the impact of IoT growth on critical infrastructures, identifying major vulnerabilities and highlighting the importance of cyber security. It also proposes solutions to address these vulnerabilities and improve the security of critical infrastructures in the IoT era. The results highlight the need for a proactive approach and good cooperation between cybersecurity and critical infrastructure stakeholders to ensure the continued operation of these indispensable systems.

The Internet of Things can be used to improve the security of critical infrastructure by implementing countermeasures and mitigating actions against potential cyber threats and vulnerabilities (M. Bures, *et al.*, 2022, 730-735*)*. Resilience is a key factor for the security of IoT systems in the context of critical infrastructures, representing an essential element in resilience to cyber-attacks and stability under optimal operating conditions (Djenna, A, *et al.*, 2021), (Hammoudeh, 2021). In order to improve cyber security systems, it is important to identify and map cyber threats, understanding the main exploitation strategies adopted by cyber criminals, thus developing specific security requirements and recommendations.

The first solution to increase the security of systems is blockchain technology. As an information storage and communication technology, based on the principles of sharing and security, which has digital data as its foundation, blockchain permanently records events in a transparent and decentralized way. In other words, a blockchain is a kind of digital ledger that stores transactions between two parties in an inviolable way. This transaction data is recorded in a network of special devices called "nodes", which is globally distributed (Hayes, 2023). The use of blockchain technology can provide secure data storage and sharing, improving the protection of critical national infrastructure (CNI) systems that rely heavily on IoT devices and physical cyber systems. By implementing blockchain technology or distributed peer-to-peer security systems, the security of IoT-enabled NCI systems can be exponentially increased.

End-to-end encryption is an important aspect of securing Internet of Things systems. It ensures the confidentiality, integrity, and authenticity of communications between endpoints and endpoints. Over time, various cryptographic protocols and algorithms have been proposed to provide secure communications in IoT devices, constrained, however, by the resources available (Jie Li, *et al.*, 2021). A pertinent example in this regard is "Sharelock", a security protocol that provides end-to-end privacy for low-cost group communication between IoT devices. It uses cryptographic primitives suitable for post-quantum cryptography and is scalable to large groups of nodes (Karbasi, *et al.*, 2020). The importance of vendors providing secure implementations of end-to-end encryption systems that respect and protect users' right to privacy needs to be emphasized (Lizardo, *et al.*, 2021), (Gurshabad, 2021).

However, security is not a priority for IoT users and there are many reasons for this. First, the resource constraints of IoT devices, such as low computing power or limited storage, make them vulnerable to cyber-attacks (Beebeejaun, *et al.*, 2023). Second, the large number of interconnected devices in IoT networks, along with the use of cloud and Wi-Fi technology, increases the risk of security attacks (Khan, *et al.*, 2023). Moreover, the lack of standard security controls or protocols for IoT devices, as well as the inability to support secure network protocols, make it difficult to implement effective security solutions (Mykhailo, *et al., 2021).*

The emergence of new service providers in the IoT ecosystem, who may not be aware of threats and security issues, further exposes the system to potential attacks (Sheeba, *et al.*, 2019). These security concerns, combined with the incompatibility of traditional mechanisms with IoT systems, contribute to users' reluctance to invest in IoT security (Santosh, 2023).

Although skepticism still covers the IoT sphere, its benefits cannot be denied, which is why many industries have adopted the Internet of Things into their operating environment.

The implementation of IoT in the automotive industry has brought many benefits and advances. IoT enables the installation of smart sensors on vehicles, allowing the use of smart applications, with a role in various services, for example: car safety, safe navigation, pollution control, or traffic management (Kuradagi, *et al., 2023*). Data security is a major concern, with threats including data leakage, theft, and tampering (Joaqong, 2022), and vulnerabilities of internet-connected industrial devices and systems, including vehicles, are often overlooked or not taken seriously (Knudsen, *et al.,* 2022). Incorporating physical cyber systems, e.g. electric vehicles, into transport networks adds new risks and challenges, including the potential for cyber-attacks targeting vehicle operating systems (Ritte, *et al.*, 2021). Addressing these security issues is essential to ensure IoT deployment in the automotive industry.

The Industrial Internet of Things (IIoT) is a growing trend in Industry 4.0, with more industrial devices and systems becoming connected to the Internet (Khan, *et al.,* 2022). Lack of security infrastructure and configurations in IoT technologies are two major concerns (Clark, *et al.*, 2023). Resource constraints in IoT infrastructures make them vulnerable to cyber-attacks and a robust security architecture is needed (Aydin, 2023). Security concerns in IoT include a lack of device updates, user awareness, software compatibility, and service disruption (Ritte, *et al.,* 2021). Lack of privacy systems in IoT systems, as well as centralized architecture, are also security risks (Kamalendu, 2021). Blockchain technology is seen as a potential solution for improving security in IoT applications.

The Internet of Things in smart homes and buildings also has many advantages but lacks a decentralized local system, which leads to serious security issues. Blockchain technology is used to overcome these problems by providing a decentralized framework and protecting data and transactions (Gaikwad, *et al.,* 2022), (Kanad, 2022). Security and privacy measures are vital in smart homes due to the importance of managing sensitive and personal data. Implementing security mechanisms compatible with IoT systems is challenging and existing security mechanisms are not adequate. Therefore, both in-depth analysis and identification of the main security gaps in IoT systems are needed. Incorporating technologies such as blockchain, artificial intelligence, and machine learning can help solve security issues in IoT systems (Srujana, *et al., 2023*), (Pannayagol, *et al.,* 2023).

The Internet of Things therefore faces significant vulnerabilities that pose security risks to both ordinary users and national security. These vulnerabilities include resource constraints, lack of security measures, outdated components, and insecure default settings (Singla, *et al., 2023*), (Ramalingam, *et al.,* 2023). Adversaries can exploit these vulnerabilities to launch cyber-attacks, gain financial benefits, and access sensitive data (Abhiskek, 2021). The lack of specific standardization in IoT technology contributes to the exposure of systems to classical attacks and illegal data collection (Harmata, 2021). In addition, there is a lack of comprehensive and focused sources of information about vulnerabilities affecting IoT devices and software (Rytel, *et al.,* 2020). These vulnerabilities and, of course, the risk of attacks on IoT networks highlight the need for robust security measures to protect national security interests.

IoT vulnerabilities can therefore have serious consequences for national security. These threats arise from vulnerabilities embedded in IoT devices, which are easily exploited by hackers who can gain remote access to systems (Anand, *et al.,* 2020). It has been found that security best practices for IoT devices are severely lacking, leading to the discovery of vulnerabilities that can be exploited for new attacks (Valente, *et al.,* 2019). The increasing number of connected devices in IoT creates more access points for intruders, increasing the risk of attacks and system hijackings (Pacheco, *et al,* 2019). Security issues can lead to damage to user facilities, prolonged downtime, and irreparable damage to capital assets (Chadid, *et al.,* 2017). Compromising the security of devices can have serious consequences, making them attractive targets for hackers (Dazine, *et al.,* 2018). To effectively address these security issues, better end-to-end security solutions are needed to protect data and ensure network privacy.

Botnets have become a major IoT security concern due to their ability to exploit vulnerabilities and launch attacks on IoT devices and networks. Various models and algorithms have been developed to detect and mitigate botnet attacks (Zhao, *et al.,* 2021). Machine learning algorithms, such as support vector machines or decision trees, have been implemented to detect botnet attacks, with tree-based algorithms achieving high accuracy rates (Wahgas, *et al., 2021*). Intrusion detection systems (IDS) have been developed to enhance the security of IoT devices, with signature-based detection schemes and trusted signature updates being used to strengthen protection against emerging attacks (Nasid, *et al.,* 2023). Scalable ecosystem-optimized security solutions are needed to address the vulnerability of IoT systems and devices to distributed denial-of-service attacks (Bertino, *et al.,* 2017).

Artificial intelligence (AI) can play an important role in detecting and mitigating botnet attacks on IoT devices, providing real-time feedback, and enabling proactive protective countermeasures (Alzahrani, *et al.*, 2022).

Mirai Botnet, a malware that launched DDoS attacks in 2016, exploited weak security measures of Internet of Things devices (Eustis, 2019). These attacks raised concerns about the lack of security for IoT devices and their potential impact on national security (Khajuria, *et al.,* 2017). The Mirai Botnet targeted critical infrastructure points, including banking systems, and launched a new form of DDoS attack that used compromised IoT devices (Jaramillo, 2018). The emergence of IoT brings new threats to information security, and the Mirai Botnet is one such threat that exploits vulnerabilities in IoT devices (Cruz, *et al.,* 2021). Researchers have developed mechanisms, techniques, and machine learning algorithms to detect and mitigate Mirai Botnet attacks on IoT networks (Snehi, *et al.,* 2021). Mirai security analysis and understanding of IoT-specific network behaviors led to the development of effective IoT-DDoS defense solutions.

Mirai is a type of malware that aims to compromise IoT devices using Linux operating systems. The aim of this malicious software is to turn these devices into parts of botnets under the control of remote attackers. Devices likely to be affected by Mirai include surveillance webcams, DVR systems, WiFi routers, and other internet-connected home devices. The Mirai botnet has been used to execute large-scale, high-impact DDoS attacks (DNSC, 2016).

Mirai took advantage of vulnerabilities present in IoT devices such as CCTV cameras and routers to achieve its goal. In October 2016, this malware orchestrated a DDoS attack against Dyn Inc., the provider of access to major platforms such as Twitter, Amazon, and Netflix. The impact of this attack was felt by consumers, who were prevented from accessing the services for several hours. While the exact financial implications are hard to estimate, the Mirai incident highlighted the vulnerability of critical services to attacks via IoT devices. States or non-state entities could use an IoT botnet to attack sectors such as healthcare, energy, transport, or a country's finances. Attacks against national critical infrastructure could have devastating consequences. While speculation in the absence of evidence is rarely wise, it is easy to see how financial services or rail networks could be affected by such attacks. While there has been no cyber-attack to date that would bring down the global financial system, the risk of such a threat is significant.

Identifying the perpetrator of a major attack is a challenge, but attribution efforts are becoming increasingly effective. If a state or terrorist group is identified as responsible for such an attack, national security agencies must act swiftly to counter the threat. For NATO member states, a cyber-attack could even trigger a collective military and political response.

Interconnectivity and the expansion of the Internet of Things have significant implications for national security. Increased connections between devices and their vulnerability to cyber-attacks can cause personal injury, property damage, and disruption to critical operations (Paul, 2019), (Dazine, *et al.,* 2018). In terms of national security, direct physical threats resulting from IoT device security issues pose an increased risk compared to conventional Internet of Things systems. (Raghuvanshi, *et al.,* 2022). The diversity of sectors involved in the Internet of Things and their influence on everyday life accentuates the seriousness of security issues as they can cause property damage, disruption, and even loss of life. (Chadid, *et al.,* 2017). Given these threats, it is important to implement comprehensive (end-to-end) security solutions that cover all aspects of connectivity and ensure data and privacy protection in IoT networks (Furnell, *et al.,* 2020). It is important to identify and mitigate security risks associated with the Internet of Things to ensure the safety and security of national critical infrastructure.

The increasing use of the Internet of Things in critical infrastructures has raised security and safety concerns due to poor engineering practices. For these IoT systems in critical infrastructures, resilience is essential, including the ability to withstand cyber-attacks, operate stably under varying conditions, and ensure reliability and safety in the face of potential failures. Appropriate countermeasures and actions need to be implemented to minimize the impact on the resilience of these systems (Djenna, *et al.,* 2021), (Hammoudeh, 2020), (Bures, *et al.,* 2022).

Governments around the world are taking various measures to ensure national security in the context of the Internet of Things. They are releasing policies, regulations, standards, and guidelines to address cybersecurity issues associated with IoT (Montasari, 2023). These policies aim to protect critical sectors, especially the security of banking, transportation, law firms, the military, academia, and hospitals from cyberattacks (Ujjan, *et al.,* 2022). In addition, governments are exploring the development of IoT security strategies to protect sensitive and confidential data from exfiltration (Gang, *et al.,* 2020). Some countries are also considering establishing a nationwide cordon to detect and filter cyber-attacks (Gosain, *et al.,* 2020). The focus is on improving transparency and reducing bias in AI algorithms used for military applications (Shu, 2010). Overall, governments are actively working to address challenges and ensure the security of IoT systems to protect national interests.

So far, both the US and the UK have avoided imposing strict regulations, preferring to put pressure on companies to develop safer products. However, these policies do not address the fundamental problem: companies continue to offer products with low levels of safety because consumers are willing to buy them. There is a balance between supply and demand. Currently, there is little incentive for companies to bring IoT products to market that meet high-security standards. In addition, within global supply chains, the situation becomes even more complex as national initiatives cannot solve transnational problems.

The market is unlikely to solve this problem, making more robust government regulation almost inevitable. Few administrations appreciate the complexity of this challenge. From a policy perspective, it is considered a "serious problem". Even if there is an obvious solution, the likelihood of its implementation is low due to the competitive motivations of key players and the rapid pace of technological change.

A more radical approach would be to consider the purpose for which the Internet of Things exists in the first place. It is the result of both laudable goals, such as energy efficiency and public welfare, and the obsession with connectivity itself. As has been shown, complex systems can generate unpredictable effects. To minimize the risks associated with global connectivity, we need to consider prioritizing devices that are truly needed over those that are simply desired. This requires a fundamental shift in mindset, with a focus on the public good over profit and political expediency.

Expanding connectivity between everyday objects brings both benefits and security risks. On the one hand, it allows a large amount of information to be collected and processed quickly. On the other hand, the increased flow of data between devices opens up new threats and opportunities for interception.

While hardware and software security measures are increasingly built into devices from the design phase, the use of strong encryption is fundamental to a secure connection between devices and the systems they rely on.

Conclusions

The Internet of Things has brought significant benefits in a number of areas, including the management of critical infrastructures by optimizing their efficiency and monitoring. However, as the use of IoT devices in these infrastructures expands, increased cyber security risks also arise. Cyber-attacks, software vulnerabilities, and unauthorized access are just some of the threats facing critical infrastructure security in the IoT era.

To manage these risks and ensure adequate protection against cyber threats, it is necessary to develop security solutions and strategies tailored to the specific needs of critical infrastructures. Implementing technical countermeasures such as end-to-end encryption, blockchain technology or distributed security solutions helps to improve the security of IoT systems in critical infrastructures.

Close collaboration between cybersecurity and critical infrastructure actors is also fundamental to the effective identification and management of cyber vulnerabilities and threats. Governments have an important role to play in national security by adopting appropriate policies and regulations to manage the risks associated with the use of IoT in critical infrastructures.

In conclusion, security in the IoT era is a major challenge, but through an interdisciplinary approach and collaboration between various stakeholders, it is possible to develop effective solutions to protect critical infrastructures and ensure their continuous and secure operation in the evolving digital environment.

BIBLIOGRAPHY:

1. Abhishek, Raghuvanshi, Umesh, Singh, Thanwamas, Kassanuk., Khongdet, Phasinam. 2021. "Internet of Things- Security Vulnerabilities and Countermeasures. ."
2. Alexander, G., Eustis. 2019. "The Mirai Botnet and the Importance of IoT Device Security." 85-89. doi:10.1007/978-3-030-14070-0_13.
3. Amir, Djenna, Saad, Harous, Djamel, Eddine, Saidouni. 2021. "Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure." *Applied Sciences, 11(10)* 4580. doi:10.3390/APP11104580.
4. Amir, Hassani, Karbasi, Siyamak, Shahpasand. 2021. "SINGLETON: A lightweight and secure end-to-end encryption protocol for the sensor networks in the Internet of Things based on cryptographic ratchets." *The Journal of Supercomputing* 77(4):3516-3554. doi:10.1007/S11227-020-03411-X.

5. André, Lizardo, Raul, Barbosa, Samuel, Neves., Jaime, Correia., Filipe, Araujo. n.d. "End-to-end secure group communication for the Internet of Things." 58:102772. doi:10.1016/J.JISA.2021.102772.
6. Antonia, Raiane, Santos, Araujo, Cruz, Rafael, L., Gomes, Marcial, Porto, Fernandez. 2021. "DIMI: Detecção Inteligente de Botnets Mirai em Redes IoT." doi:10.14210/COTB.V12.P362-369.
7. 2023. "Car to Car Communication using IoT." *International Journal For Multidisciplinary Research* 5(4). doi:10.36948/ijfmr.2023.v05i04.4195.
8. Chaobin, He. 2022. *Vulnerabilities and new critical security challenges of the Internet of Things (IoT).* doi:10.1016/b978-0-323-85174-9.00009-1.
9. Colin, Tankard. 2015. "The security issues of the Internet of Things." *Computer Fraud & Security, 2015(9)* 11-14. doi:10.1016/S1361-3723(15)30084-1.
10. Devashish, Gosain, Madhur, Rawat, Piyush, Kumar, Sharma., Hrishikesh, B., Acharya. 2020. "Maginot Lines and Tourniquets: On the Defendability of National Cyberspace." 19-30. doi:10.1109/LCNSYMPOSIUM50271.2020.9363273.
11. 2022. "E-Government Privacy and Security Challenges in the Context of Internet of Things." 22-42. doi:10.4018/978-1-7998-9624-1.ch002.
12. Elisa, Bertino, Nayeem, Islam. 2017. "Botnets and Internet of Things Security. IEEE Computer. IEEE Computer, 50(2)." 76-79. doi:10.1109/MC.2017.62.
13. Eugen, Wendler. 2022. "Hybrid deep-learning model to detect botnet attacks over internet of things environments. Soft Computing, 26(16)." 7721-7735. doi:10.1007/s00500-022-06750-4.
14. 2022. "Factors Impacting Resilience of Internet of Things Systems in Critical Infrastructure." doi:10.1109/aiiot54504.2022.9817259.
15. Gang, Zhanhui, Chang-Yue, Yu, Huang, Haibo, Wang, Lijun. 2020. "Research on International and Domestic Internet of Things Security Policy." doi:10.1109/ITCA52113.2020.00115.
16. Gurshabad, Grover, Olaf, Kolkman, Mallory, Knodel, Fred, Baker., Sofia, Celi. 2021. "Definition of End-to-end Encryption."
17. Hao, Zhao, Hui, Shu, Ying, Xing. 2021. "A Review on IoT Botnet." doi:10.1145/3448734.3450911.
18. 2022. "Implementation of Blockchain Technology in IOT Based Smart Home." doi:10.1109/icast55766.2022.10039525.
19. 2023. "Internet of Things Based Smart Home Security Analysis System." doi:10.1109/iceconf57129.2023.10083624.
20. 2022. "Internet of Things: Security Vulnerabilities and Countermeasures 107(1):15043-15052." doi:10.1149/10701.15043ecst.
21. James, Wenceslaus, Ritte. 2021. "Security Concerns in Internet of Things." *International Journal for Research in Applied Science and Engineering Technology, 9* 2898-2901. doi:10.22214/IJRASET.2021.36977.
22. Jiaqing, Shi, Yaping, Yang., Shiyi, Wang. 2022. "Internet of vehicles data security risks and protection." doi:10.1117/12.2634508.
23. Jihad, Dazine, Abderrahim, Maizate., Larbi, Hassouni. 2018. "Internet of things security." doi:10.1109/ITMC.2018.8691239.
24. José, Custodio, Najar-Pacheco., John, Alexander, Bohada-Jaime., Wilmar, Yovany, Rojas-Moreno. 2019. "Vulnerabilities in the internet of things 13(2)." 312-321. doi:10.14483/22484728.15163.
25. Junia, Valente, Matthew, A., Wynn., Alvaro, A., Cardenas. 2019. "Stealing, Spying, and Abusing: Consequences of Attacks on Internet of Things Devices. 17(5)." 10-21. doi:10.1109/MSEC.2019.2924167.

26. Kamalendu, Pal. 2021. *Blockchain With the Internet of Things: Solutions and Security Issues in the Manufacturing Industry.* doi:10.4018/978-1-7998-5839-3.CH009.
27. Kanad, Gaikwad., Kaustubh, Kulkarni., Surekha, Kohle., Pradnya, Patil. 2022. "Implementation of Blockchain Technology in IOT Based Smart Home." 6-10. doi:10.1109/ICAST55766.2022.10039525.
28. 2022. "Lightweight Internet of Things Device Authentication, Encryption, and Key Distribution Using End-to-End Neural Cryptosystems." *IEEE Internet of Things Journal* 9(16):14978-14987. doi:10.1109/jiot.2021.3067036.
29. Luis, Eduardo, Suástegui, Jaramillo. 2018. "Malware Detection and Mitigation Techniques: Lessons Learned from Mirai DDOS Attack." *Journal of Information Systems Engineering and Management, 3(3)* 19. doi:10.20897/JISEM/2655.
30. Manish, Snehi, Abhinav, Bhandari. 2021. "Apprehending Mirai Botnet Philosophy and Smart Learning Models for IoT-DDoS Detection." 501-505. doi:10.1109/INDIACOM51348.2021.00089.
31. Marcin, Rytel., Anna, Felkner., Marek, Janiszewski. 2020. "Towards a Safer Internet of Things-A Survey of IoT Vulnerability Data Sources." *Sensors, 20(21)* 5969. doi:10.3390/S20215969.
32. M'Kaila, J., Clark., Lila, Rajabion. 2023. "A Strategic Approach to IoT Security by Working Towards a Secure IoT Future." *International journal of hyperconnectivity and the Internet of Things, 7* 1-18. doi:10.4018/ijhiot.317088.
33. Mohammad, Hammoudeh. 2020. *Blockchain, Internet of Things and Digital Twins in Trustless Security of Critical National Infrastructure.* doi:10.1145/3440749.3442650.
34. Muhammad, Hassan, Nasir., Junaid, Arshad., Muhammad, Mubashir, Khan. 2023. "Collaborative device-level botnet detection for internet of things. Computers & Security, 129." 103172-103172. doi:10.1016/j.cose.2023.103172.
35. Muhammad, Waqas., Kamlesh, Kumar., Asif, Ali, Laghari., Umair, Saeed., M., M., Rind., Aftab, Ahmed, Shaikh., Fahad, Hussain., Athaul, Rai., Abdul, Qayoom, Qazi. 2021. "Botnet attack detection in Internet of Things devices over cloud environment via machine learning. Concurrency and Computation: Practice and Experience." doi:10.1002/CPE.6662.
36. Mykhailo, Hunko., Igor, Ruban., Kateryna, Hvozdetska. 2021. *Securing the Internet of Things via VPN technology.* doi:10.30837/CSITIC52021232903.
37. P., Srujana., Kalluri, Rama, Krishna., S., Madhavi., Chhavi, Sharma., N., Satheesh., G., Poshamallu. 2023. "Internet of Things Based Smart Home Security Analysis System." 1-6. doi:10.1109/ICECONF57129.2023.10083624.
38. Paul, C., van, Oorschot., Sean, W., Smith. 2019. "The Internet of Things: Security Challenges 17(5)." 7-9.
39. Pooja, Anand., Yashwant, Singh., Arvind, Selwal. 2020. "Internet of Things (IoT): Vulnerabilities and Remediation Strategies." doi:10.1007/978-981-15-8297-4_22.
40. Reza, Montasari. 2023. "Artificial Intelligence and the Internet of Things Forensics in a National Security Context." *Advances in information security* 57-80. doi:10.1007/978-3-031-21920-7_4.
41. Santosh, L., Deshpande. 2023. "Security in Internet of Things: An Overview." 243-248. doi:10.1109/DICCT56244.2023.10110070.
42. 2022. "Security at the Internet of Things." 31-48. doi:10.1201/9781003220985-3.
43. 2023. "Security in Internet of Things." In *Security in Internet of Things. Advances in information security, privacy, and ethics book series*, 215-233. doi:10.4018/978-1-6684-6914-9.ch011.
44. 2022. "Security in Internet of Things." 99-117. doi:10.1201/9781003337812-6.

45. 2023. "Security in Internet of Things. Advances in information security, privacy, and ethics book series." 215-233. doi:10.4018/978-1-6684-6914-9.ch011.
46. 2023. "Security in Internet of Things: An Overview." doi:10.1109/dicct56244.2023.10110070.
47. 2022. "Security in the Industrial Internet of Things." 119-134. doi:10.1201/9781003337812-7.
48. Sheeba, Backia, Mary, Baskaran., Sivabalan, Arumugam., Anand, Raghawa, Prasad. 2019. "Internet of Things Security." 7(1):21-42. doi:10.13052/JICTS2245-800X.712.
49. Shu, Jun. 2010. " Security Crisis and Countermeasures of Internet of Things. China Public Security, ."
50. Vani, Rajasekar., S., Rajkumar. 2023. "A Study on Internet of Things Devices Vulnerabilities using Shodan." *International Journal of Computing* 149-158. doi:10.47839/ijc.22.2.3084.
51. Yassine, Chahid., Mohamed, Benabdellah., Abdelmalek, Azizi. 2017. "Internet of things security." 1-6. doi:10.1109/WITS.2017.7934655.
52. Khan, W.A., Rahman, K., Hussain, G., Abbas, G., & Wang, X. (Eds.). (2023). Machine Tools: An Industry 4.0 Perspective (1st ed.). CRC Press. https://doi.org/10.1201/9781003220985oi:10.1109/WITS.2017.7934655.

1053477-3045-1396-24-43

HYBRID WARFARE AND CRITICAL INFRASTRUCTURES PROTECTION

Mr. Cezara ȘOIMU
Master Officers, Specializing in Joint Leadership, Air Force
Air Force Department, Faculty of Command and Staff
"Carol I" National Defence University, Bucharest, Romania
E-mail: clara.iris@yahoo.com

Cpt. cdor. Ciprian BERAR
Master Officers, Specializing in Joint Leadership, Air Force
Air Force Department, Faculty of Command and Staff
"Carol I" National Defence University, Bucharest, Romania
E-mail: cip_luck@yahoo.com

Cpt. cdor. Marcel PETROV
Master Officers, Specializing in Joint Leadership, Air Force
Air Force Department, Faculty of Command and Staff
"Carol I" National Defence University, Bucharest, Romania
E-mail: marcel_marcel80@yahoo.com

Abstract: *This article delves into the intricate realm of hybrid warfare and its profound impact on critical infrastructures. Hybrid warfare, characterized by a blend of conventional, irregular, and cyber tactics, presents a multifaceted threat to national security. The paper begins by defining hybrid warfare, underscoring its evolution and the complexity of its modern manifestations. It then systematically identifies and examines the key components of hybrid warfare, including cyber-attacks, information warfare, economic pressure, and the utilization of non-state actors. The focus shifts to critical infrastructures, outlining their definition, significance, and inherent vulnerabilities susceptible to hybrid threats.*

Through comprehensive analysis, the article highlights how these infrastructures, pivotal to a nation's functioning and security, become targets in this new age of warfare. To provide a practical perspective, case studies are presented, showcasing instances where critical infrastructures have been compromised, followed by an examination of the responses and mitigation strategies employed.

The crux of the discussion lies in proposing robust protection strategies. These encompass technological solutions, policy interventions, and international collaborative efforts, aimed at fortifying infrastructures against the ingenuity of hybrid threats. The article concludes by addressing the ongoing challenges and projecting future trends in hybrid warfare tactics, emphasizing the need for adaptability and proactive defense mechanisms in safeguarding critical national assets.

Keywords: *hybrid warfare, critical infrastructure, vulnerabilities, protection, challenges*

Introduction to Hybrid Warfare

The evolution of warfare has been marked by a continuous adaptation to changing political, technological, and social landscapes. From the conventional conflicts characterized by direct, state-on-state military engagements, warfare has progressively incorporated more complex and subtle forms of conflict. The advent of guerilla tactics and insurgency during the 20th century, exemplified in conflicts such as the Vietnam War, marked a shift towards irregular warfare. This shift was further augmented by the rise of terrorism and non-state actors, adding a new dimension to the battlefield (Frank Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars, 2007, p. 85).

The emergence of hybrid warfare in the 21st century represents a culmination of this evolution. Hybrid warfare blurs the lines between conventional and unconventional, regular and irregular, military and civilian. It combines a range of tactics - from cyber-attacks, disinformation campaigns, and economic pressure, to the use of proxy forces. These tactics are employed in a strategic manner to exploit vulnerabilities, often aiming to destabilize and coerce without triggering a full-scale conventional response. The Russo-Georgian War of 2008 and the ongoing conflict in Ukraine are prime examples of hybrid warfare in action (Mary Kaldor, New and Old Wars: Organized Violence in a Global Era, 2012, p. 103).

This transformation reflects the adaptability of state and non-state actors to leverage technological advancements and societal vulnerabilities, signifying a shift in the nature of global conflict and necessitating new defense and security strategies.

Based on recent scholarly articles, the most comprehensive definition of hybrid warfare can be derived as follows: *Hybrid warfare is a multifaceted form of conflict that blends a variety of conventional and unconventional, regular and irregular, and cyber and physical tactics. This form of warfare is characterized by its adaptability, the use of a wide range of political, military, economic, and social means, and a deliberate blurring of the lines between war and peace, combatants and civilians. It often involves the use of proxy forces, misinformation campaigns, cyber-attacks, and economic pressure to achieve strategic objectives. Hybrid warfare exploits vulnerabilities within the opponent's societal, political, and economic systems, often with the aim of destabilizing and coercing while avoiding attribution or direct confrontation.*

This definition synthesizes the key elements found in recent studies and expert analyses on the subject, capturing the essence of how hybrid warfare is understood in contemporary security and strategic discourses.

1. Key Components of Hybrid Warfare

The key components of hybrid warfare include, among other means, cyber-attacks, propaganda, economic pressure, and the use of irregular armed forces.

Cyber warfare forms a critical component of hybrid warfare, involving the use of computer technology to disrupt the information systems of the enemy. These attacks target critical infrastructures like power grids, communication networks, and national security apparatus. An example is the 2007 cyber-attacks against Estonia, where government, media, and banking websites were overwhelmed with service denials, significantly disrupting the nation's digital infrastructure.

Propaganda. Information warfare, another pillar of hybrid warfare, involves the use of propaganda to influence public opinion and destabilize societies. This is achieved through disinformation, fake news, and social media manipulation. A notable instance is Russia's alleged interference in the 2016 U.S. presidential election, where social media platforms were reportedly used to spread disinformation and influence voter perceptions.

Economic measures, such as sanctions, trade embargoes, and financial manipulation, are employed to weaken an adversary's economy. These tactics aim to create political and social unrest, thereby exerting pressure on governments without military engagement. The ongoing U.S.-China trade war, characterized by the imposition of tariffs and economic sanctions, exemplifies this aspect of hybrid warfare.

The use of irregular armed forces in hybrid warfare often involves the use of proxy forces, militias, and private military contractors to achieve military objectives without direct state involvement. This approach provides plausible deniability while achieving strategic goals. The Syrian Civil War presents an example, where various external powers have supported different factions and militias, complicating the conflict and its resolution (The U.S. Department of Defense, 2018).

Historically, hybrid warfare tactics have been evident in conflicts like the Vietnam War, where guerrilla tactics, political propaganda, and conventional warfare were combined. More recently, the annexation of Crimea by Russia in 2014 showcased a sophisticated blend of unmarked military personnel, local militias, propaganda, and cyber warfare, effectively achieving strategic objectives without engaging in large-scale conventional warfare (Timothy Snyder, The Road to Unfreedom: Russia, Europe, America, 2018, p. 65).

In conclusion, hybrid warfare represents the evolution of conflict in the modern era, marked by the strategic combination of diverse tactics. This approach exploits the interconnected nature of global systems and societies, presenting new challenges for national and international security frameworks.

Critical infrastructures refer to the physical and cyber-based systems and assets that are essential to the functioning of a society and its economy. These infrastructures are pivotal for maintaining national security, economic vitality, and public health and safety. They include sectors such as energy, water supply, transportation, banking and finance, telecommunications, health care, food production and distribution, and emergency services (The U.S. Department of Homeland Security, 2018).

The importance of critical infrastructures lies in their interconnectedness and their role in supporting all aspects of modern life. The disruption of any one of these infrastructures can have cascading effects on others, leading to widespread societal impact. For example, a failure in the power grid can affect water supply, healthcare services, communication networks, and transportation systems. This interdependency underscores their significance in ensuring the smooth functioning of a nation.

Energy infrastructure, encompassing power generation, transmission, and distribution systems, is fundamental for running industries, businesses, and homes. It powers other critical infrastructures, making it a primary target for attacks aimed at crippling an economy. Also, water and wastewater systems are crucial for public health. Contamination or disruption of these systems can lead to immediate and severe health crises.

Speaking about transportation, this would include air, rail, water, and road networks. Transportation infrastructure is vital for the mobility of people and goods, impacting economic activity and access to essential services. Another important sector is banking and finance which underpins economic stability. Attacks on financial systems can erode public trust and cause significant economic disruptions.

Communication networks are essential for the dissemination of information and coordination during emergencies. Cyber-attacks on these systems can isolate individuals and organizations. In addition, hospitals and health systems are vital for public welfare. Their incapacitation can lead to loss of life and hinder disease control efforts and related to that the food sector ensures the availability of necessary nourishment. Disruption can lead to shortages, panic, and social unrest.

Last but not least, emergency services which include law enforcement, firefighting, and emergency medical services, are crucial for public safety and order (Ted G. Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, 2006, pp. 87-88).

Critical infrastructures are thus not only assets but also systems that underpin national security, economic stability, and public welfare. Their protection against both physical and cyber threats is paramount to ensure national resilience against a range of challenges, including natural disasters, technological failures, and deliberate attacks. The safeguarding of these infrastructures is a national priority, requiring coordinated efforts between governments, private sector entities, and the public to mitigate risks and enhance security.

2. Vulnerabilities of Critical Infrastructures

Critical infrastructures, despite their crucial role in national security and public welfare, possess inherent vulnerabilities that can be exploited by hybrid warfare tactics. These vulnerabilities stem from various factors, including technological dependencies, interconnectedness, and the evolving nature of threats.

Many critical infrastructures rely heavily on digital technologies and cyber systems for their operation. This reliance creates vulnerabilities to cyber-attacks, such as hacking, malware, and denial of service attacks. For example, the 2015 cyber-attack on the Ukrainian power grid, which left hundreds of thousands without electricity, highlighted the vulnerability of energy infrastructures to cyber threats (Kaspersky Lab, 2016).

The interdependent nature of critical infrastructures means that disruption in one can have cascading effects on others. This interconnectedness can be exploited to amplify the impact of an attack. In 2017, the WannaCry ransomware attack affected over 200,000 computers across 150 countries, disrupting various sectors including healthcare, where it severely impacted the UK's National Health Service (National Cyber Security Centre UK, 2017)

Besides cyber threats, physical attacks on infrastructure components like power lines, transportation hubs, or water treatment facilities can cause significant disruption. The sabotage of Saudi Arabia's Khurais oil facility in 2019, which temporarily cut off half of the country's oil production, illustrates this vulnerability (BBC News, 2019).

Insider Threats: Employees or contractors with access to infrastructure systems can pose a significant threat if they are coerced, compromised, or act maliciously. Insider threats can lead to both physical and cyber breaches.

Supply Chain Vulnerabilities: Many infrastructures depend on complex, often global, supply chains. Disruption or manipulation of these supply chains can have direct impacts on infrastructure functionality.

Exploitation in Hybrid Warfare: Hybrid warfare tactics can exploit these vulnerabilities in a coordinated manner. Cyber-attacks can be used to gather intelligence, disrupt communications, or directly damage infrastructure systems. Disinformation campaigns can exacerbate the impact of physical or cyber-attacks by spreading panic or misinformation. Economic measures, such as sanctions or trade restrictions, can strain the resources needed to maintain or protect infrastructures.

In hybrid warfare, the targeting of critical infrastructures serves not just to cause immediate disruption but also to achieve broader strategic objectives like weakening adversary states, undermining public confidence, and exerting political pressure. The protection of these infrastructures requires a multi-layered approach involving physical security, cybersecurity, supply chain risk management, employee vetting, and international cooperation.

3. Protection Strategies

Protecting critical infrastructures from hybrid threats involves a multi-faceted approach that integrates technology, policy-making, and international cooperation. These strategies and measures are designed to fortify infrastructures against a wide array of threats, ranging from cyber-attacks to physical sabotage.

Implementing advanced cybersecurity measures is paramount. This includes the use of firewalls, intrusion detection systems, and regular security audits to identify and mitigate vulnerabilities. The deployment of encryption technologies ensures data integrity and confidentiality. Furthermore, developing and integrating resilient systems that can isolate and contain attacks to prevent them from spreading is essential. For example, the use of AI and machine learning can enhance threat detection and response capabilities (National Institute of Standards and Technology, 2018).

Regular risk assessments help identify potential threats and vulnerabilities. This involves analyzing the likelihood and impact of various threat scenarios and implementing measures to mitigate these risks. It also includes the development of contingency and disaster recovery plans to ensure rapid response and restoration of services in case of an attack. Governments play a crucial role in establishing robust regulatory frameworks to protect critical infrastructures. This includes setting standards for cybersecurity, physical security, and emergency preparedness. Policies should also encourage information sharing between public and private sectors about threats and best practices. For instance, the implementation of the EU's NIS Directive aims to raise the level of security of network and information systems across the EU (European Union Agency for Cybersecurity, 2020).

Regular training for employees on security protocols and threat awareness is critical. Additionally, programs to identify and mitigate insider threats are necessary, as personnel with access to critical systems can be a significant vulnerability. Hybrid threats often transcend national borders, making international collaboration essential. This includes sharing intelligence, and best practices, and cooperating in investigations and responses to incidents. Collaborative efforts through organizations like NATO, the European Union, and INTERPOL enhance collective defense capabilities against hybrid threats (NATO, 2019).

Many critical infrastructures are owned and operated by the private sector. Therefore, building strong partnerships between government and industry is essential for effective protection strategies. These partnerships facilitate coordinated responses, resource sharing, and the development of unified security standards.

In conclusion, protecting critical infrastructures from hybrid threats requires a holistic approach that combines advanced technology, comprehensive policy frameworks, rigorous risk management, employee training, international cooperation, and public-private partnerships. Such a multi-layered defense strategy is vital to ensure the resilience and security of these essential assets.

4. Case Studies

4.1. 2015 Ukrainian Power Grid Cyber Attack

In December 2015, Ukraine's power grid experienced a significant cyber-attack, which is one of the first known successful cyber-attacks on a power grid. Hackers, believed to be Russian state-sponsored, infiltrated the grid's control systems and caused a blackout affecting approximately 230,000 people for several hours.

In the attack analysis, it was concluded that the attackers used spear-phishing emails to install "Black Energy" malware in the power company's computer systems. They gained access to the control systems of three electricity distribution companies and shut down substations. The attack was sophisticated, involving coordinated efforts across different regions.

The Ukrainian power companies responded by switching to manual operation, a contingency plan for cyber-attacks. This quick response helped restore power within a few hours. Post-attack, Ukraine strengthened its cyber defenses by upgrading its cybersecurity protocols and systems, conducting regular employee training sessions to recognize phishing attempts, implementing strict access controls to their systems, and increasing international cooperation with European and U.S. cybersecurity entities for knowledge and resource sharing (Kim Zetter, 2022).

This incident underlined the vulnerability of critical infrastructures to cyber-attacks and the importance of having robust cybersecurity measures and effective emergency response protocols.

4.2. 2019 Attacks on Saudi Arabian Oil Facilities

In September 2019, Saudi Arabia's oil facilities at Abqaiq and Khurais were attacked, significantly disrupting global oil supplies. The Houthi rebels in Yemen claimed responsibility, but the U.S. and Saudi Arabia attributed the attack to Iran, marking it as an instance of hybrid warfare involving physical and possibly cyber elements.

The attack was carried out using a combination of cruise missiles and drones, which bypassed Saudi Arabia's air defenses. This indicated a high level of sophistication and planning. The choice of targets demonstrated a strategic aim to disrupt the global oil supply and impact the Saudi economy. The immediate response involved firefighting and emergency management services to control the fires and prevent further damage and rapid repair and restoration operations to bring oil production back online.

For long-term mitigation, Saudi Arabia and its allies considered strengthening air defense systems against drone and missile attacks while increasing intelligence and surveillance operations to detect and prevent future attacks. Also, measures were taken to enhance physical security measures at critical infrastructure sites and explore diplomatic channels to address the regional tensions underlying such attacks

This case emphasized the complexity of defending against hybrid warfare tactics, where physical attacks are combined with potentially other forms of aggression, requiring a multi-dimensional approach to security and defense (BBC News, 2019).

4.3. The 2010 Stuxnet Attack on Iran's Nuclear Program

The Stuxnet attack, discovered in 2010, represents a landmark in cyber warfare history. It targeted Iran's nuclear program, specifically the Natanz uranium enrichment facility, and is widely believed to have been developed by the United States and Israel. Stuxnet was one of the first known cyberattacks that caused physical destruction to industrial equipment.

Attack Analysis. Stuxnet was a highly sophisticated computer worm designed to specifically target Siemens Step7 software used in industrial control systems. It exploited multiple zero-day vulnerabilities (flaws in software that are unknown to the vendor) and spread through infected USB drives. Once inside the system, Stuxnet sought out Siemens Programmable Logic Controllers (PLCs), which are used to automate industrial processes. Its primary objective was to manipulate the centrifuges used for uranium enrichment: it subtly altered the rotational speed of the centrifuges, causing physical damage while simultaneously sending normal operation data to the monitoring systems, thus concealing the attack (Ralph Langner, 2011).

The response to the discovery of Stuxnet included removal of the malware from infected systems and patching the vulnerabilities it exploited, increased security measures around industrial control systems, particularly those in sensitive facilities, and enhanced monitoring of network activities to detect anomalies indicative of such sophisticated attacks.

For long-term mitigation and to prevent similar incidents, there was a global realization of the need for improved cybersecurity protocols for industrial control systems with a greater collaboration between industrial firms and cybersecurity experts to safeguard critical infrastructure followed by the development of national and international guidelines and policies for the protection of critical infrastructure against cyber threats (Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, 2014, pp. 63-65).

The Stuxnet case was significant for several reasons. It marked the first time a cyberattack caused significant physical damage to a critical infrastructure, illustrating the potential of cyber weapons to impact the physical world. It also highlighted the vulnerability of industrial control systems to cyber threats, which was a wake-up call for cybersecurity in industrial sectors worldwide. Additionally, the sophistication and apparent state sponsorship of Stuxnet signified a new era in cyber warfare capabilities and strategies.

These case studies illustrate the diverse nature of hybrid warfare attacks on critical infrastructures and the importance of a multi-faceted response and mitigation strategy, also serve as stark reminders of the evolving nature of threats to critical infrastructures and the need for continuous adaptation and enhancement of defense and security measures.

They highlight the need for strong cybersecurity measures and contingency plans, regular training and awareness programs for personnel, robust physical security and air defense systems, international cooperation, and intelligence sharing and diplomatic efforts to address underlying geopolitical tensions.

5. Challenges and Future Trends

The ongoing challenges in protecting critical infrastructures are multifaceted, stemming from the evolving nature of threats, technological advancements, and the increasing interconnectedness of global systems. One of the primary challenges is the sophistication of cyber threats. As attackers develop new techniques and exploit emerging technologies like AI and machine learning, the complexity and frequency of cyberattacks are expected to increase. This necessitates continuous updates and advancements in cybersecurity measures (James A. Lewis, The Future of Cybersecurity: Trends and Challenges in Protecting Critical Infrastructure, 2018, p. 47).

Another significant challenge is the integration of legacy systems with modern technologies. Many critical infrastructures operate on outdated systems that are not designed to withstand current cyber threats, making them particularly vulnerable. Upgrading these systems is often costly and complex.

The insider threat remains a persistent challenge. Employees with access to critical systems pose a potential risk, either through malicious intent or inadvertent errors. Strengthening insider threat detection and management is crucial.

Regarding future trends in hybrid warfare tactics, it is likely that we will see an increase in the use of cyber capabilities to achieve strategic objectives without traditional military engagement. Cyberattacks may be used more frequently to cause physical damage to infrastructure, disrupt economic activities, and spread disinformation. The use of autonomous systems and drones in hybrid warfare is also expected to rise, offering new means for surveillance and targeted attacks.

The use of misinformation and deepfakes powered by AI technology is anticipated to become more sophisticated, posing challenges to information integrity and public trust. Additionally, the blurring of lines between state and non-state actors in cyber operations could lead to increased ambiguity in attribution, complicating international response and policy-making (Andy Greenberg, Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers, 2019, p. 68).

In conclusion, the protection of critical infrastructures requires a dynamic and adaptive approach, integrating advanced technology, comprehensive policy frameworks, and international cooperation. The future of hybrid warfare tactics will likely involve a blend of cyber, physical, and psychological elements, necessitating a holistic and resilient defense strategy.

Conclusion

In this article, we have explored the multifaceted and evolving landscape of hybrid warfare and its significant impact on critical infrastructures. Hybrid warfare, defined as a strategic blend of conventional, irregular, cyber, and other tactics, represents a modern threat paradigm that challenges traditional notions of conflict and security. We have dissected the key components of hybrid warfare, including cyber-attacks, propaganda, economic pressure, and the use of irregular armed forces, each contributing to the complex nature of these threats.

Critical infrastructures, the backbone of national security and public welfare, have been identified as prime targets in this new age of warfare. Their inherent vulnerabilities, stemming from technological dependencies, interconnectedness, and other factors, open avenues for exploitation by hybrid warfare tactics. We examined notable instances, such as the 2015 Ukrainian power grid cyberattack and the 2019 attacks on Saudi Arabian oil facilities, providing insights into the challenges faced and the mitigation strategies employed.

The protection of these vital systems calls for robust strategies encompassing technological solutions, policy interventions, and international collaborative efforts. Addressing the ongoing challenges in this realm, such as the sophistication of cyber threats and the integration of legacy systems with modern technologies, is imperative. Furthermore, the article has highlighted the importance of proactive measures and adaptability in policy and defense strategies, particularly in light of the predicted future trends in hybrid warfare tactics, which include increased use of cyber capabilities, autonomous systems, drones, and advanced disinformation campaigns.

In conclusion, the evolving nature of hybrid warfare necessitates a dynamic and comprehensive approach to safeguard critical infrastructures. It underscores the need for continuous technological advancement, policy evolution, international cooperation, and a holistic defense strategy to effectively counter these multifaceted threats. The protection of critical infrastructures is not only about securing assets but also about preserving the societal, economic, and political stability of nations in the face of sophisticated and evolving threats.

BIBLIOGRAPHY:

1. Andy, Greenberg. 2019. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York: Knopf Doubleday Publishing Group.
2. Frank, G., Hoffman. 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, Virginia: Potomac Institute for Policy Studies.
3. Kim, Zetter. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown Publishers.
4. Mariarosaria, Taddeo and Ludovica, Glorioso. 2017. *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative*. Switzerland: Springer Cham.
5. Mary, Kaldor. 2012. *New and Old Wars: Organised Violence in a Global Era*. Stanford University Press.
6. Ted, G., Lewis. 2006. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. New Jersey: John Wiley and Sons, Inc.
7. Timothy, Snyder. 2018. *The Road to Unfreedom: Russia, Europe, America*. New York: Tim Duggan Books.
8. James, A., Lewis. 2018. ”The Future of Cybersecurity: Trends and Challenges in Protecting Critical Infrastructure.” Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/0601_cscip_preliminary.pdf

9. Kim, Zetter. 2022. ”What We Know and Don’t Know about the Cyberattacks Against Ukraine - (updated).” https://www.zetter-zeroday.com/what-we-know-and-dont-know-about/
10. Myriam, Dunn, Cavelty and Manuel, Suter. 2009. ”Public-Private Partnerships are no silver bullet: An expanded governance model for critical infrastructure protection.” International Journal of Critical Infrastructure Protection. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1997145
11. Ralph, Langner. 2011. ”Stuxnet: Dissecting a Cyberwarfare Weapon.” IEEE Security and Privacy. https://ieeexplore.ieee.org/document/5772960
12. ”Summary of the 2018 National Defense Strategy of The United States of America.” 2018. The U.S. Department of Defense. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf
13. ”Dhs Resilience Framework. Providing a roadmap for the Department in Operational Resilience and Readiness.” 2018. U.S. Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/dhs_resilience_framework_july_2018_508.pdf
14. ”TLP: White. Analysis of the Cyberattack on the Ukrainian power grid.” 2016. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf
15. ”The cyber threat to UK bussines.” 2017. National Cyber Security Centre UK. https://www.ncsc.gov.uk/files/NCA%20Report_17_18.pdf
16. ”Saudi Arabia oil attacks: Weapons debris 'proves Iran behind them' ”. 2019. BBC News. https://www.bbc.com/news/world-middle-east-49746645
17. ”Framework for Improving Critical Infrastructure Cybersecurity.” 2018. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf
18. ”EU Cybersecurity Act and NIS Directive”. 2019. European Union Agency for Cybersecurity (ENISA). https://eur-lex.europa.eu/eli/reg/2019/881/oj
19. ”Countering hybrid threats”. 2023. North Atlantic Treaty Organization (NATO). https://www.nato.int/cps/en/natohq/topics_156338.htm

1053477-3045-1396-24-44

SECURITY OF CRITICAL INFRASTRUCTURE: AN INTEGRATED APPROACH TO PROTECTING VITAL RESOURCES

Nicoleta MOLDOVAN-PUI
Second lieutenant, ”Carol I” National Defense University, Bucharest, Romania
E-mail: nicoletamoldovan1@yahoo.com

Abstract**:** *Critical infrastructures represent the ensemble of facilities, services, and systems that are essential for the functioning of modern society. Strengthening and maximising the capabilities of all elements that make up critical infrastructures is at the core of contemporary debates at national level from a security perspective and at European and global level from an international security perspective. In the current century, critical infrastructures are much more sensitive in terms of vulnerability in the context of cyber security. Today, we are facing a future laden with uncertainties, and discussing the security of critical infrastructures can become a rather challenging task, especially since modern conflict is characterized by geopolitical, social, economic, technological, environmental, and military influences. However, sudden and unforeseen changes in society, technological developments or political developments are not always taken into account. In what follows, some topical issues of everyday life will be brought to the fore, which, by extension, are considered to be cogs in a larger system, while the minuses, shortcomings and potential threats will be addressed.*

Keywords: *critical infrastructure, security, cyberattacks, conflict.*

Introduction

The early emergence of critical infrastructure became notable long ago. It commenced after an extended period when ancient civilizations began to flourish in various fields of activity and became aware of the "value" of an asset. Consequently, they deemed it opportune to develop a system of fortifications at the expense of security. So, in the 18th century, there were communication and transport infrastructures whose main defining feature was interconnections and interdependencies at a limited level. This has led to the emergence of wide vulnerabilities in the context of local critical infrastructures.

Starting from the 20th century and continuing into the current century, we are witnessing unprecedented technological advancement and the intensification of globalisation. With the proliferation of computers and the Internet, they have become the foundation of essential infrastructures such as, for example: the global financial system. The interdependencies and connections between these infrastructures expand on an intercontinental scale, and the emergence of non-state actors and the concept of supranationality (reflected in the existence of entities such as the European Union, the International Monetary Fund, etc.) contribute to the expansion of vulnerabilities globally.

Critical infrastructures from a defining perspective

In an increasingly interconnected world with a heightened dependence on technology, critical infrastructures play a vital role in ensuring the daily functioning of humanity. The services provided by critical infrastructures are essential for society, thus necessitating the need for their protection and the establishment of their resilience capacity (Rinaldi, Peerenboom and Kelly, 2001). These include transportation networks, energy systems, communications, critical facilities, and key points in the geographic area. They form the backbone of modern society and provide essential services, often perceived as guaranteed.

However, with the increasing alertness of human dependence, a new category of threats is emerging, becoming more and more sophisticated. It is desirable to adopt an integrated approach to protect these vital resources and ensure safe operation. The decision of the States to designate critical infrastructures at the national level and to legislate for their protection has generated inter-institutional dialogue, promoted the training of specialists in the field and facilitated collaboration between entities (Pătrașcu, 2019, 44). At the same time, simulations were organised to assess the resilience of critical infrastructures in different sectors of activity. The protection of Critical Infrastructures is regulated and substantiated legislatively, based on Emergency Ordinance no. 98, from 2010, regarding the determination, clear establishment, and provision of necessary support to elements with a pronounced sensitive character, revised/updated by Law no. 225, from August 1, 2018. The current legislative framework outlines the vital functions and designates them as: "*those services that are essential for the functioning of society, such as: government business management, international activities; national defense; internal security; the functioning of the economy and infrastructure; the security of the population's income and standard of living*" (Law 225/2018).

Critical infrastructures are divided into 12 sectors, according to this law, and each sector is under the aegis of a state institution. The fact that critical infrastructures belong to the maintenance of the state of normality of society obliges national security institutions to resort to methods of limiting public access to tools with a highly sensitive level of information content. These actions emphasize the need to strengthen data security, which can impact the smooth conduct of daily activities and pose a potential threat to the integrity and stability of the state.

Therefore, by identifying and assessing potential threats, implementing appropriate security measures, and developing rapid response protocols in case of incidents, risks are significantly reduced, ensuring the safe operation of these vital infrastructures.

Cyber influences in the context of CI

One of the greatest threats to critical infrastructures is posed by cyberattacks. Hackers and cybercriminal groups may attempt to compromise systems and cause significant damage. By implementing robust cybersecurity measures, such as data encryption, constant monitoring, and regular system updates, the risk of these attacks can be reduced, safeguarding critical infrastructures (Steingartener, Galinec and Kozina, 2021, 4).

The characteristics of the information environment, in the context of the digital age, allow different entities to use information activities to disseminate information and engage audiences according to their own objectives. At the same time, the development of technologies, access to the internet and the presence on social networks in increasing numbers have led to the scale of effects impacting the cognitive dimension, which at any moment could trigger a conflict without a direct physical confrontation.

In recent years, digital technologies have fundamentally changed the way people are exposed to and interact with information. The Internet has made it possible to create content at low cost and distribute it to ever larger audiences. Social networks blurred the boundaries between personal and mass communication, and search engines have enabled a vast amount of information instantly and often freely accessible on a large scale.

In the modern era, critical infrastructure (CI) vulnerability is a major and complex concern. With advanced technologies and global interconnectivity, CI become exposed to various threats, including sophisticated cyberattacks, extreme natural events and geopolitical challenges. Managing CI vulnerabilities requires innovative approaches and continuous adaptability, integrated within global strategies that promote resilience, international cooperation and implementation of security best practices. Constant vigilance and sustained investment in technologies and expertise are essential to anticipate and counter emerging threats, thereby ensuring the continuous operation and security of critical infrastructures in the evolving landscape of the 21st century.

The sheer number of attacks is too extensive for human analysts to combat efficiently, but advanced artificial intelligence techniques can greatly improve the capabilities of analysts and experts to counter the adversary in this regard. The swift deployment of these methods is now more viable than ever.

Regarding cybersecurity, anomaly detection applications can be developed to enhance analysts' ability to monitor extensive networks and respond quickly to incidents.

Similarly, in actions involving a potential cyberattack, information gathering can be accomplished by analyzing the adversary's communication systems and identifying valuable information that could influence the process of countering or neutralizing the attack in a timely manner, without causing significant damage to the target by a potential attacker (Buță, 2023). Thus, by creating rigorously outlined policies, it is possible to create an internal - own decision-making protocol.

Modern conflicts have demonstrated that both conventional and unconventional forces use new generation methods of influence, including "deepfakes", via the internet, which has resulted in messages to target audiences arriving in a very short time frame requiring verification of the veracity of information from multiple sources. Time is an important factor and is gaining ground on the content of the messages, which means that any reaction is delayed and less effective than what we are accustomed to. Information is being picked up at a rapid pace and the digital battlespace is starting to grow.

Methods adopted by EU to combat cyber threats

On 1 December 2012, the European Agency for the Management of Large-scale IT Systems in the area of Freedom, Security and Justice (eu-LISA) started its operational activity. Located in Tallinn, the Agency manages the Schengen Information System (SIS II), the Visa Information System (VIS) and the Eurodac system, thus contributing significantly to ensuring security within the Schengen area.

The European Cybercrime Centre, also known as EUROPOL, was established in 2013, with the aim of providing support for effective law enforcement action to combat cybercrime within the European Union.

Since its inception, the centre has been involved in multiple high-profile cases, providing on-scene support for hundreds of successful arrests and analyzing hundreds of thousands of files as part of its analytical work. Every year, EUROPOL produces an IOCTA report containing key observations on cybercrime recorded during that period, including the emergence of new threats. Within the organisation, the entity known as the Cyborg Focal Point, is tasked with countering high-tech crime that poses threats, in particular, to critical infrastructures in Europe.

In conclusion, it can be seen that there are entities operating at Union level with the task of combating, preventing and stopping this type of threat of the present century.

The phenomenon of globalisation

Globalisation is a process by which countries, people and cultures around the world establish more interconnected and interdependent relationships. This phenomenon manages to maintain its character of continuous novelty, facilitated by advances in technology, transport and communications. With globalisation, goods, services, information and even ideas can move more easily across the world. This can bring benefits such as access to products and technologies with innovative impact, openings to business opportunities and cultural exchanges. However, like any large-scale phenomenon, globalisation can also have challenges, such as instability, thus creating economic inequalities, job losses in certain sectors and environmental impacts.

To provide a conclusive perspective, it is pointed out that this phenomenon had and continues to have a significant impact on critical infrastructure, because they are often globally interconnected. For example, communication and transport networks are vital to facilitate the exchange of information, goods and services between different countries. Also, energy infrastructures are essential to secure energy supplies in a globalised world.

The globalisation of the information environment has made it increasingly difficult to analyse and evaluate it, forcing entities to put more effort and train their IT staff, in order to have high-performance analysts and meet the requirements for monitoring and identifying false accounts and information. Social media has also gone viral and allow rapid distribution of messages of any kind to a number of people unheard of before the digital age, bringing to the fore the need to have a warning system supporting entities/large establishments to react in a timely manner so that the desired effects are achieved.

Due to the rapid evolution of technology, as a society, we must adapt in a short time to new methods of influence and attack used by potential adversaries, to have modern monitoring equipment and constant evaluation of the effects produced in order to be able to refine in time the control methods adopted in the initially proposed plans.

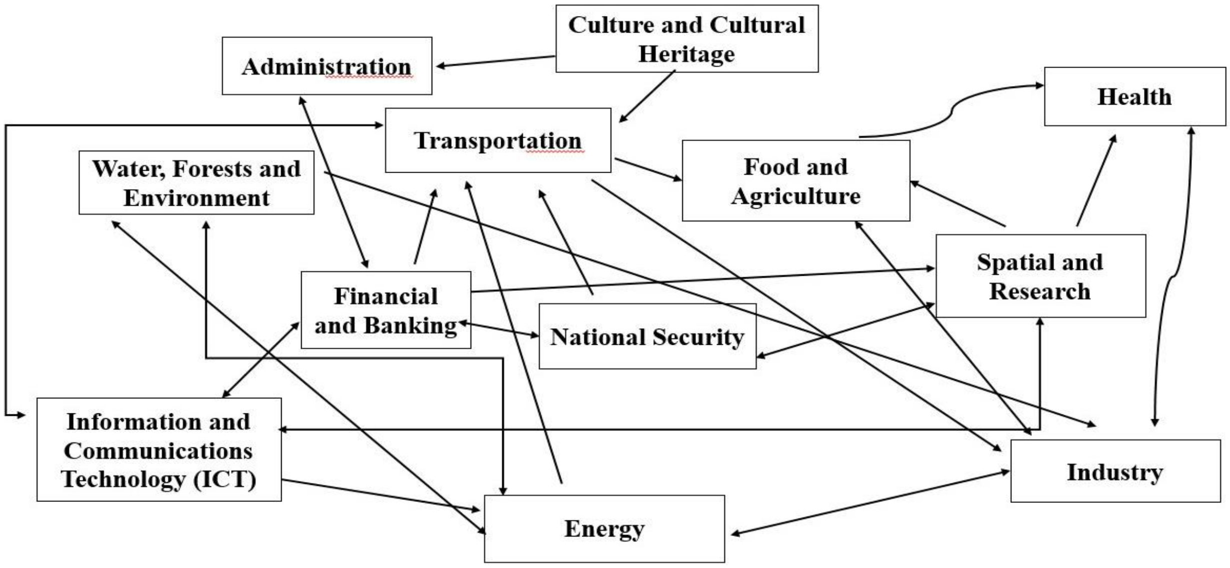


Figure no. 1. Interdependencies among sectors

Adapting to global requirements is a significant feature in the context of globalisation. As interconnectedness and interdependence become increasingly present, both companies and organisations, as well as individuals, are required to show flexibility and adjust to global requirements and directions. This may involve understanding and respecting cultural diversity, adapting to international standards and regulations, showing openness to collaboration and the use of advanced technologies to meet requirements at a broad level. So, accommodating to global demands can be a challenge, but at the same time can generate opportunities for expansion and progress.

Methods adopted to protect CI at EU level

The constantly innovative nature of the 21st century requires, both directly and indirectly, decision-making institutions to implement measures.

On 17 November, in 2005, The Commission has introduced a new reference document regarding a European Programme for Critical Infrastructure Protection, entitled "Green Paper”. This document formulated three strategies in the defence sector, with the main line of activity being the enhanced mitigation of threats of all kinds. This document includes the five principles (subsidiarity, complementarity, cooperation, confidentiality, proportionality), which are integral components of Directive 2008/114/EC (Nitra, 2017).

On the 16th and 17th of December, 2004, The European Council validated the European Programme for Critical Infrastructure Protection (EPCIP), initiated by the European Commission, and gave the green light for the establishment of the Warning Network for Critical Infrastructures (CIWIN). EPCIP was designed to ensure a consistent and adequate level of protection for critical infrastructures within the European Union. It is necessary to periodically reassess the EPCIP, to adapt to new requirements and risks. To ensure these adaptations, it is essential to adhere to the following principles:

- ❖ ***The principle of subsidiarity***, which implies that the protection of critical infrastructures is primarily the responsibility of member states, focuses on European Critical Infrastructures (ECI). It efficiently complements existing measures by consolidation through an additional level of support provided by EPCIP.
- ❖ ***The principle of confidentiality*** imparts a crucial characteristic, as information related to critical infrastructures holds particular importance for their proper functioning, constituting a facilitating factor in the context of successful cyberattacks. This principle also holds a paramount position concerning the exchange of information relevant to the protection of critical infrastructures.

EPCIP is structured around three defining workflow streams. The first of these represents a national framework for the development of strategies and the establishment of horizontal measures, while the second focuses on the protection of European Critical Infrastructures (ECI). The third stream is designed to assist member states in ensuring the security of critical infrastructures.

The mention of the European Reference Network for Critical Infrastructure Protection (ERNCIP) project is essential, this has been established as an implementation tool for the protection of critical infrastructures, with a particular emphasis on implementing EPCIP.

By promoting cross-border collaboration, implementing international standards, and adopting advanced technologies, the EU succeeds in creating a resilient and interconnected framework, essential for the vital protection of critical infrastructures in the complex landscape of the 21st century.

Methods adopted for the protection of Critical Infrastructure at the national level

Based on a public statement from a national institution operating in the field of national information and telecommunications protection (STS), it is mentioned that the improvement and consolidation of the protection capacity of critical infrastructures is a prominent topic discussed within European forums dedicated to security, both as an integral part and as an imperative measure for the national security of Romania.

In light of the current geostrategic context and security issues, along with the visible impact of an ongoing conflict in the proximity of Romania's borders, the adoption of an approach that accentuates fidelity to reality regarding the role of critical infrastructures and essential services becomes imperative. These are vital not only for the efficient functioning of the economy and society as a whole but also for ensuring the defense of the country and national security.

In the management and operation of critical infrastructures at the national level, as well as in providing essential services within its area of competence, The Special Telecommunications Service has adapted to an increasingly complex and aggressive security context. It has adopted innovative approaches in implementing digitization solutions, placing particular importance on the implementation of fundamental principles such as "security by design" or "privacy by design" since the conceptualization stage.

Considering that threats in the field of communications and information technology often have different sources or vectors, the institution comprehensively assesses all potential risks and orients itself towards resilience covering the seven levels of the Open Systems Interconnection (OSI) model: the physical, logical, network, transport, and session levels, the presentation and application levels, in accordance with the suggestions outlined in Directive NIS 2.

The efficiency and accessibility of a critical infrastructure or essential service are strongly influenced by the performance of interconnected components. Therefore, it is essential that all these elements adhere to the same high standards regarding development, quality, and security.

The intensified dynamics of threats, whether cyber or non-cyber in nature, highlight the fact that attackers do not precisely apply a rigorous selection of targets. It is assumed that IT&C infrastructures do not enjoy the level of security we might presume, and encryption, although essential for data protection, cannot serve as the sole line of defense. In other words, monitoring one's own infrastructures is a priority for establishing robust security, The continuous adaptation of protection plans to a high level, as well as their immediate implementation.

The expertise of national professionals active in the field forms the basis upon which national strategies are built. Allocating all necessary resources with the ultimate goal of securing the infrastructure, adapted to contemporary requirements, must be supported by state institutions with such expertise in the field. Therefore, periodic vulnerability assessments and simulation exercises contribute to the efficient identification and remediation of potential weaknesses in protection systems. Continuous investment in advanced security technologies and innovative research in the field is essential to keep pace with evolving threats and effectively counter new risks.

Conclusions

The current context of modern conflicts is closely tied to the expansive developments of the present century, shaping advanced forms of threats. In the cyber realm, whether at a local or global level, it has a widespread impact on the security of critical infrastructure. It is imperative that the process of influencing or raising awareness of desired perceptions in this context be based on studies and information with an impact on the audience, shaped long before the onset of the virtual conflict, and have long-lasting effects so that the informational support and prominent security of the actors do not affect human operations/actions or even lead to a reduction in lethal actions.

This study has brought to attention the main elements of critical infrastructure. This paper outlines in broad strokes, with a defining emphasis, the infrastructures, followed by the cyber threats to them that can give rise to conflicts with a significant impact on society. We have highlighted the methods implemented by the European Union to counter cyber threats and addressed the fundamental phenomenon of the globalization process. Furthermore, we considered it opportune to shed light on the subject of critical infrastructure protection at the European and national levels within the legislative sphere, identifying the main reference documents.

Nowadays, we can affirm that warfare has a volatile and changing nature and can take various forms, ranging from conventional high-intensity conflicts between equal (or nearly equal adversaries) up to counterterrorism or counterinsurgency operations and even reaching a level of conflict conducted in the digital sphere. The evolution of security risks and the volatile nature of conflicts have unequivocally allowed for an appropriate adaptation of the capabilities of Alliance members. After the 9/11 moment, the NATO military community directed its attention and resources toward the threats and insecurity generated by terrorist groups, engaging its forces in counterterrorism and counterinsurgency operations, as well as in stability missions. The Russian invasion of Crimea in 2014 led to a shift in the paradigm and priorities, prompting NATO member countries to readjust their military capabilities for large-scale conflicts. The recent, unprovoked war by Russia against Ukraine somewhat justified these resizing and adjustments of capabilities but also serves as a harsh reminder that a large-scale war among European nations is still possible (Fridbertsoon, 2022, 1).

In the report *"Technological Innovation for Future Warfare",* NATO Parliamentary Assembly rapporteur Njall Trausti Fridbertsson (Iceland) mentions current trends that characterize and shape conflicts and wars today. Thus, he mentions *"the fluidity of the transition from conflict to large-scale war, the role of non-state actors, urbanization, climate change," as well as "progress and access to cutting-edge technologies" (*Fridbertsoon, 2022, 1*).* Last but not least, data and digitization at the level of infrastructures represent a true game-changer in current conflicts.

In conclusion, it is important to consider that owners or operators of critical infrastructure may have connections with the private sector, and since ensuring security requires significant financial investments, cost optimization in terms of security expenses is not allowed, thus playing a key role in this regard are the state authorities and institutions at the European level. In the contemporary era, with the evolution of both state and non-state actors adopting new hybrid tactics (Weels, 2022, 6), to advance their interests, the concept of protecting critical infrastructure has gained increased importance, particularly regarding resilience capacity. Currently, the majority of security incidents unfold in the cyber domain.

BIBLIOGRAPHY:

1. Buță, Ionuț-Cosmin, Arilie 2023, Resilience of critical infrastructures in the context of cyber insecurity caused by hybrid threats, National University of Defense „Carol I", 3.
2. David E. Whitehead, Kevin Owens, Dennis Gammel, Jess Smith, March 2017, Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies, în Power and Energy Automation Conference Spokane, Washington, 3.
3. Fridbertsson, Njall Trausti, November 2022, Tehnological Innovation for Future Warfare, Bruxelles, adopted by the NATO Parliamentary Assembly, 10.
4. Pătrașcu, Petrișor, March 2019, Cyber Actions Against Critical Infrastructures in the Military Field, Bulletin of the National University of Defense „Carol I".
5. Steingartner William, Darko Galinec, Andrija Kozina, April 2021, „Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model", Symmetry, 2021, 13 (3): 597.
6. Steven M. Rinaldi, James P. Peerenboom, Kelly, Terrence K., December 2001, "Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies." IEEE Control System Magazine, 2001, 21(6): 11-25.
7. Schmitt M., Tallinn, 2017, Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd Edition. Prepared by the International Group of Experts at the invitation of NATO CCDCoE. Cambridge University Press,12-15.

8. Wells, John S. G., September 2022, „Preparing for Hybrid Warfare and Cyberattacks on Health Services' Digital Infrastructure: What Nurse Managers Need to Know", Journal of Nursing Management, 30 (6): 2000-4.
9. *** Law no. 225/2018 amending and supplementing Government Emergency Ordinance no. 98/2010 regarding the identification, designation, and protection of critical infrastructure, is available on the internet at the following address: https://legislatie.just.ro.
10. „Homepage", European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), disponibil la dresa: https://www.europol.ruropa.eu/about-europol/european-cybercrime-centre-ec3.
11. „Homepage", European Cybercrime Centre – EC3, disponibil la adresa: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.
12. Internet Organised Crime Threat Assessment (IOCTA), Europol, Haga, 2020, disponibil la adresa https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020
13. https://eur-lex.europa.eu/RO/legal-content/glosarry/green-paper.html
14. https://www.europarl.europa.eu/deceo/document/A-7-2012-0167_RO.html
15. https://erncip-project.jrc.ec.europa.eu
16. https://sts.ro/ro/protectia-infrastructurilor-critice-si-rezilienta-din-perspectiva-sts/

1053477-3045-1396-24-45

LEGAL AND OPERATIONAL FRAMEWORK OF CRITICAL INFRASTRUCTURES' PROTECTION IN ROMANIA

Andreea MIHALCEA
Bucharest, Romania
E-mail: andreea26mihalcea@gmail.com

Alexandru ȘUHAN
Bucharest, Romania
E-mail: alex.suhan10@gmail.com

Abstract: *The study analyzes Romania's framework for protecting critical infrastructures, emphasizing the impact of Government Emergency Ordinance no. 98/2010, which lays the foundation for their protection. It distinguishes between National Critical Infrastructures (ICN) and European Critical Infrastructures (ICE), underlining their importance for national security and societal functions. The text highlights the roles of stakeholders in maintaining infrastructure security and resilience, stressing the need for a strong legal and operational framework to protect against disruptions and align with EU and NATO standards.*

Keywords: *Critical Infrastructures Protection, Resilience, Legal Framework, National Security, European Union Directives*

The complexity of systems developed in the modern era has generated the imperative of meticulous regulation for all aspects within a society. In order to ensure fair treatment for all citizens, common and individual rules of law have been introduced, outlined in a legislative framework. In the initial stage, any emerging sector or field is often characterized by the absence of regulations, a phenomenon that leads to increased risks due to the lack of legal guidance. Along with the development of critical infrastructures, the need for rigorous regulation of this field was imposed, along with the establishment of a legislative framework adapted to the efficiency of the protection process of these vital infrastructures.

The need to protect critical infrastructures has been recognized at European Community level, especially following the events of September 11 in the United States. As a result, the European Union adopted a series of regulations, to which the member states and those aspiring to join, including Romania, complied. In the following pages, we will briefly present the evolution of the legislative framework regarding the protection of critical infrastructures at the European level, in order to better understand the regulatory directions that have also influenced the Romanian legislation in this regard.

In 2004, the Council of Europe requested the development of a global strategy for the protection of critical infrastructures, resulting in two reference documents for this field: "The European Union Solidarity Program in the Consequences of Terrorist Threats and Attacks" and "Communication on the Protection of Critical Infrastructures in within the framework of the fight against terrorism". As a result of these, in 2005 the "Green Card on the European program for the protection of critical infrastructures" was adopted, concluding that there must be more institutions to deal with the protection of these infrastructures, through inter-state cooperation. Next, to improve their ability to achieve security, the Council of the European Union adopted the "C.E. Directive no. 114/2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection" (DIRECTIVA 2008/114/CE), within which it operates its own definition of critical infrastructures.

At the level of the Romanian state, the protection of critical infrastructures is an activity that falls within the European framework, having the following characteristics (Rizea, 2010):

- Integration into the North Atlantic Alliance (hereafter referred to as NATO) and the European Union (hereafter referred to as the EU) should require the adaptation of a national legislative framework that converges towards the European idea of protecting critical infrastructures;
- Interconnection of Romanian and European critical infrastructures, in order to be able to participate in the European exchange market, but also to share resources and know-how;
- Combating activities that may endanger critical infrastructures, activities such as terrorism, organized crime or various types of illegal traffic, to strengthen EU and NATO security;

The first legislative approach in Romania appeared 2 years later, by issuing "Government Emergency Ordinance no. 98 of November 3, 2010 on the identification, designation and protection of critical infrastructures". Within this GEO, it started by specifying the role of critical infrastructures for a state, namely having roles both at the economic and social level and from the perspective of citizens' security. The respective Government Emergency Ordinance is the legislative basis for regulating the field of critical infrastructure protection at the level of the Romanian state.

This GEO appeared in the context of the need to transpose "Directive 2008/114/EC" into national legislation and to create the primary regulation related to the field of critical infrastructures in national legislation, which can support the development of programs and access to European funds which can be used in the field of critical infrastructure protection.

One of the first important elements within GEO 98/2010 was the definition of critical infrastructures at the level of the Romanian state, these being defined as follows: "an element, a system or a component thereof, located on the national territory, which is essential for maintaining the functions vital aspects of society, health, safety, security, social or economic well-being of individuals and the disruption or destruction of which would have a significant impact at national level as a result of the inability to maintain those functions, as well as the project of a strategic objective of national interest whose construction is imperatively necessary to safeguard the national interest". The critical infrastructures in Romania were named as "National Critical Infrastructures" (abbreviated ICN), being compared to the "European Critical Infrastructures" (abbreviated ICE) to which the national ones are interconnected through the various systems that operate at the international level.

Prior to the publication of this emergency ordinance that would specifically and clearly regulate the issue of a normative framework for achieving the protection of critical infrastructures, similar concepts were used as meaning. The first legislative references in the normative acts of the Romanian state regarding the definition of critical infrastructures can be found in the following documents:

- *The National Strategy for Prevention and Countering of Terrorism (2002) – stated that there are certain infrastructures that keep the social life of community and that can be targets of terrorist attacks;*
- *The national strategy for the sustainable development of Romania (2004) – infrastructures that can be included in sustainable development programs to maintain a high level of quality in the public sector, especially in the future, are described and listed here;*

- *Law no. 535 on the prevention and combating of terrorism (2004) – contains elements that today we recognize as critical infrastructures were defined as objectives of strategic importance;*
- *Order no. 660 of the Minister of Economy and Trade, regarding the approval of the Guide for the identification of critical infrastructure elements in the economy () - normative act in which critical infrastructures are presented as "objectives of particular importance existing within the national economy*" (Rizea, 2010);
- *National Security Strategy of Romania* (2006) – adopted by the Supreme Council of National Defense (hereinafter referred to as CSAT), in the text we find the enumeration of some infrastructures of major interest in the field of state security, and critical infrastructures are those that have an effect, as we will see, on this field. (National Security Strategy of Romania, 2006*)*

As seen, with the publication of GEO 98/2010, the normative framework for achieving the protection of critical infrastructures was clearly established, emphasizing their interconnectivity, but also the two forms of critical infrastructures: ICN and ICE. The author considers that the terms European critical infrastructure and national critical infrastructure become relative in the context of the increasingly visible interconnection of critical infrastructures in recent years and the dependencies that have appeared at the European, but also international level, thus taking into account within the PEPIC program and the need giving importance to all critical infrastructures, regardless of their type.

Considering the way in which these types of infrastructures interact with each other, subordinate or superordinate each other, it can be said about critical infrastructures, both national and European, that they "form a robust system with multiple interdependencies, constantly diversifying, within which the vector of information technology plays a crucial role" (Badea, 2015). The development of modern infrastructures, as systems within states to provide different services, utilities or to satisfy important social needs, has been based on technological evolution and the creation of supply chains and systems that require their interconnection in order to operate these complex processes that to lead to today's functioning of these infrastructures that we call critical.

We can thus see the importance for security of maintaining critical infrastructures in a functional state, a task that is both the operators and administrators of these infrastructures, as well as the state and the citizens of the state. This importance has led to the norming of critical infrastructure protection (hereinafter referred to as PIC). By applying the PIC, according to GEO 98/2010, the following elements are ensured for critical infrastructures:

- Functionality – this characteristic refers to the maintenance of a system in which all components work harmoniously to continue to provide outputs from that infrastructure, thereby ensuring the essential societal functioning of that infrastructure. Any deviation from the functional state of critical infrastructures must be corrected to avoid threats to state security;
- Continuity of services – this dimension is vital not only for modern lifestyle aspects, but also for ensuring the continuous operation of the separate components of the national critical infrastructure supersystem, thus guaranteeing the continuity of essential services;
- Integrity – maintaining the integrity of critical infrastructures is a fundamental objective of Critical Infrastructure Protection (PIC), indicating that they have not suffered physical or other damage that could stop the provision of services to citizens and the state.;
- Neutralization of risks, threats and vulnerabilities – given the importance of critical infrastructures for national security, it is necessary to apply the principles of the theory

of the security of states and systems. It is essential to identify and neutralize risks, threats and vulnerabilities within specific PIC processes.

The protection of critical infrastructures is an important element in achieving the security of a state, so not only the legislation touched on the issue of the role and importance of PIC in security. In this sense, the author Cârdei Alin specifies that the protection of critical infrastructures is a component of guaranteeing the security of citizens, and specifies a series of measures that must be taken to ensure PIC: "preventing incidents, deterring threats, by implementing a robust security system, adopting passive defense measures, which amplify the constructive capacities and those due to the environment, the adoption of active defense measures, through the implementation of adapted protection systems, which have the ability to detect, prohibit, defeat the threat and, last but not least, increasing the capacity to mitigation, to minimize the effects on personnel, assets, systems, processes, population, environment and information" (Cîrdei, 2019).

It is obvious that not only the knowledge and definition of critical infrastructures and their role in society are aspects that require regulation and an adequate institutional framework. It is also imperative to develop rules and regulations that actively support the work of maintaining the continuous provision of critical infrastructure services through the implementation of Critical Infrastructure Protection (PIC). These services are essential aspects for the functioning of a modern state.

The importance of PIC for the state and civil society imposes the need for a regulation on a working framework of state institutions for the operational implementation of PIC. Thus, in the current legislation, an operational framework of the institutions responsible for ensuring the protection of critical infrastructures and, in general, managing the various aspects of this critical field has been outlined.

Following the regulation by Government Ordinance of the field of critical infrastructures, it was considered necessary to draw up a National Strategy regarding the protection of critical infrastructures. This strategy was published by "Government Decision number 718 of July 13, 2011 for the approval of the National Strategy regarding the protection of critical infrastructures". The purpose of this strategy is to establish the framework for the effective implementation of the PIC, and the elements targeted by the strategy are the following (H.G. 718/2011):

- The element of continuous development of the PIC field – given the technological development, but also the socio-political-economic movements of today, the risks to critical infrastructures vary and change even within a few years, so it is necessary, for maintaining the security of ICN and ICE, so that the field of PIC continues to develop;
- The element of regularization of internal regulations with international ones – because national critical infrastructures are interconnected with European ones and, in a wider sense, with international ones, it is necessary to harmonize regulations to optimize the processes of achieving PIC, maintaining security and maintaining functionality these infrastructures;
- The element of the involvement of all parties with interests and responsibilities related to critical infrastructures – in order to be able to carry out the PIC activity effectively, it is necessary that all institutions and actors that have a role in this field participate in the realization of protection, but also in the development to new means to form resilience for critical infrastructures to potential risks that may arise;

On these directions of action, a series of objectives were established to help quantify the degree of achievement of the PIC at the level of the Romanian state, the objectives being these (H.G. 718/2011):

- Creation of unitary ICN/ICE identification procedures;

- Development of a national system with a warning role in preventing threats or minimizing the damage caused;
- Evaluation of the degree of vulnerability of the ICN and intervention to reduce these vulnerabilities;
- Coordination of actions and relationships met at local, regional and global level in order to achieve the PIC;

Taking into account these objectives, the strategy proposes a series of directions of action, which can be summarized by the following main direction of action in the field of PIC: Development of an inter-institutional, national and European effort to implement legislative measures and find operational solutions in order to minimizing risks, avoiding threats and correcting critical infrastructure vulnerabilities. The effort coordinates of these directions of action are the following: "prevention, reduction and limitation of the effects; response/intervention; sustainability" (H.G. 718/2011).

In order to establish the operational aspects related to critical infrastructures, in the years following the publication of GEO 98/2010, a series of regulations were published with a role in clarifying the specifications of the emergency ordinance, thus resulting in the decision on the actual implementation of the PIC field at the level of the Romanian state. An important regulation in this regard was the one previously presented, namely "Government Decision number 718 of July 13, 2011 for the approval of the National Strategy regarding the protection of critical infrastructures", however, before the publication of that decision, "Government Decision no. 1110 of November 3, 2010 regarding the composition, duties and organization of the Interinstitutional Working Group for the protection of critical infrastructures". This structure with a very important operative role is subordinated to the state counselor appointed by the prime minister to deal with the executive part of the PIC issue, together with the CNCPIC within the M.A.I.

This working group is defined as a structure made up of specialist representatives in various fields related to critical infrastructures or within which critical infrastructures have been identified (H.G. 1110/2010):

- Representatives from the ministry in charge of managing the economy;
- Representatives from the ministry responsible for communications, education, research, youth issues;
- Representatives from the Ministry of Health;
- Representatives from the ministry responsible for the environment;
- Representatives from the intelligence services: Foreign Intelligence Service, Romanian Intelligence Service, Special Telecommunications Service;
- Defense representatives;
- Representatives from the field of transport;
- Other specialists with roles in the various national systems that include/use critical infrastructures.

Next, for the operationalization of the actual identification activity of the national critical infrastructures, a government decision was issued regarding the critical thresholds related to some criteria that determine the identification of ICN, it being HG 1154/2011. The national legislation continued to regulate this field, for which H.G. was issued. 1198/2012 on the "designation of national critical infrastructures", regulation amended and supplemented several times over the years. At the same time, the legislative framework in Romania makes this country one of the first in Europe that "defined its responsibilities for the people involved in the protection of critical infrastructures"(Adrian Vilciu, 2014), designation made through the issuing of "Government Decision no. 35 of January 30, 2019 for the designation of public authorities responsible for the protection of national and European critical infrastructures". This list has been established for both ICN and ICE.

In Romania, the CNCPIC within the MAI had a crucial role in the management of the Protection of Critical Infrastructures (PIC), coordinating the drafting of draft laws, provisions and implementing concrete actions to minimize risks to national critical infrastructures. CNCPIC has developed programs aimed at increasing the awareness and involvement of civil administrators in the management of these critical infrastructures.

The operational structure for achieving the PIC in Romania involves a collaboration between two entities subordinate to the public administration, but integrated in distinct organizational charts: CNCPIC and the Interinstitutional Working Group. These two governmental structures have the responsibility to implement the necessary measures for the effective implementation of the PIC, contributing, at the same time, to the development of a framework adapted to the realities and needs specific to Romania in terms of the protection of critical infrastructures.

At the present time, in Romania there is both a legal framework with the role of regulating the field of critical infrastructure protection, and an operational framework through which concrete measures are taken both for the realization of the PIC and for the awareness of the importance of these measures for national security and for the life of citizens as it is currently known.

BIBLIOGRAPHY:

1. Badea, Dorel, *Protecția infrastructurilor critice – structuri și funcționalități integratoare*, Editura Academiei Forțelor Terestre „Nicolae Bălcescu”, Sibiu, 2015.
2. Cîrdei, Ionuț Alin, *Aspecte privind protecția și reziliența infrastructurilor critice*, Editura Academiei Forțelor Terestre „Nicolae Bălcescu”, Sibiu, 2019.
3. Rizea, Marian, Enăchescu, Daniela, Neamțu-Rizea, Cristiana, *Infrastructuri critice*, Editura Universității Naționale de Apărare „Carol I”, București, 2010.
4. H.G. 1110/2010 privind componența, atribuțiile și modul de organizare ale Grupului de lucru interinstituțional pentru protecția infrastructurilor critice.
5. H.G. 35/2019 pentru desemnarea autorităților publice responsabile în domeniul protecției infrastructurilor critice naționale și europene.
6. H.G. 718/2011 pentru aprobarea Strategiei naţionale privind protecţia infrastructurilor critice.
7. http://www.ingr.ro/ro/i--Ny0x.html, accesed at 11.01.2024.
8. https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32008L0114&from=EL, accesed at 03.12.2023.
9. https://home-affairs.ec.europa.eu/system/files/2019-07/20190723_swd-2019-308-commission-staff-working-document_en.pdf, accesed at 07.01.2024.
10. http://www.ingr.ro/ro/i--Ny0x.html, accesed at 11.01.2024.
11. *Strategia de Securitate Națională a României*, București, 2007.

1053477-3045-1396-24-46

IDENTIFICATION OF THE ESSENTIAL SECTORS AND SERVICES WITHIN THE FRAMEWORK OF CRITICAL INFRASTRUCTURES IN ROMANIA

Alexandru ȘUHAN
”Carol I” National Defense University, Bucharest, Romania
E-mail: alex.suhan10@gmail.com

Andreea MIHALCEA
”Carol I” National Defense University, Bucharest, Romania
E-mail: andreea26mihalcea@gmail.com

Abstract: *The study focuses on protecting Romania's critical infrastructures, identifying essential sectors such as energy, ICT, water, health, and transport. It outlines criteria for determining an infrastructure's criticality, including indispensability, vulnerability, and functionality. The research concludes with a legislative process for safeguarding these vital sectors, emphasizing the importance of robust evaluation and protection to ensure national security and public welfare.*

Key words: *Critical Infrastructure Protection, Essential Services, National Security, Romania, Sector Evaluation*

In today's context, critical infrastructure protection (CIP) has become an essential area of research and implementation, reflecting the increasing reliance on interconnected systems and technologies. This complex field involves various processes, policies and technologies developed to ensure the security of elements and systems considered vital to the efficient functioning of modern societies. These critical infrastructures include electricity grids, transportation systems, water and gas supply infrastructures, and communications networks. In this context, research on the identification of essential sectors and services within critical infrastructures in Romania becomes crucial, representing an effort directed towards strengthening national security and protecting the vital pillars of society.

In order to classify these systems as "critical" or "conventional", the infrastructures must undergo an evaluation process based on certain criteria. These essential criteria for identifying critical infrastructures include the following assumptions (Rizea, 2008):

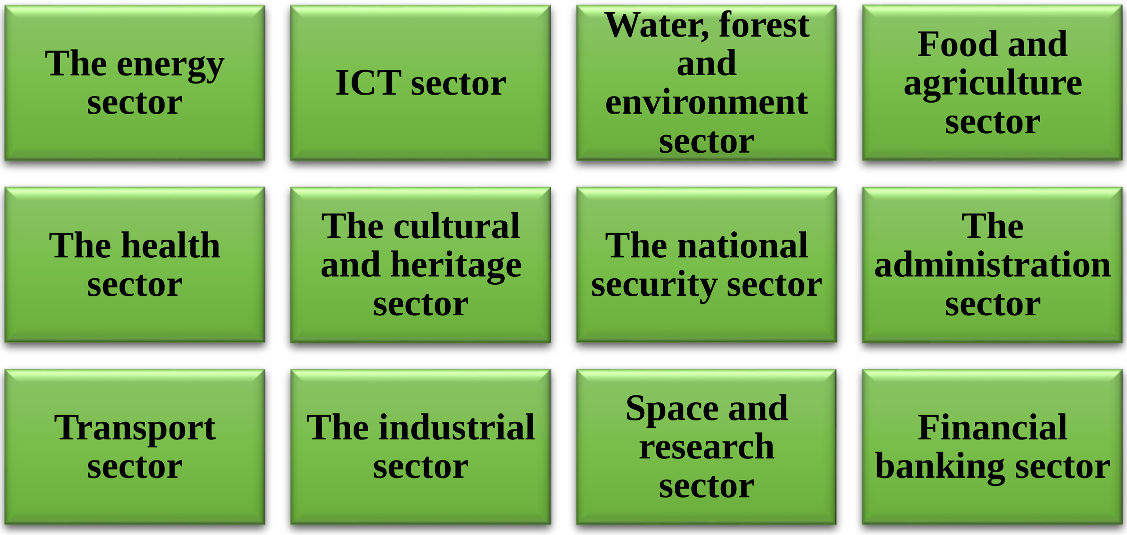
- A distinct condition exists when providing services to the citizens of a state such that these services are not available by other means and their presence and operation are critical because they provide an essential good that cannot be obtained otherwise.
- It plays a crucial role in ensuring the safety, reliability and security of systems. Critical infrastructure contributes to the stability and functionality of the entire state system. Even though some components may seem less essential in modern life, they depend on the interconnectedness of critical infrastructures mutually developed within modern states.
- It is susceptible to direct threats or disruptions to the processes within which it operates, presenting a significant vulnerability.
- It exhibits a high sensitivity to variations in the parameters in which it operates, requiring specific conditions to maintain its functionality.

It is not enough that various systems possess these characteristics to varying degrees to be considered critical infrastructure. The process of identification and classification of essential services and sectors, within which there are elements of critical infrastructure in Romania, requires the establishment of appropriate evaluation criteria. Through the analysis of the specialized literature in this field, the following evaluation criteria of the criticality of the infrastructures are highlighted (Alexandrescu, 2006):

- Physical Presence: This criterion focuses on the actual physical existence of infrastructure elements as compared to other components of the national infrastructure. The assessment takes into account how these elements interact with each other and contribute to the overall stability of the national infrastructure.
- Functionality: The functional criterion focuses on the specific role of the infrastructure within the national or international context. The government services or sectors covered by that critical infrastructure and its impact on their proper functioning are analyzed.
- System Security: The evaluation of the system security criterion takes into account how the functionality or non-functionality of the respective infrastructure affects the security of the state system. The risks and impact on national integrity and security are analyzed.
- Unpredictability: The criterion of unpredictability explores the idea that, under special circumstances, some sectors may move from a normal state to a critical one. Infrastructures in these sectors can consequently become critical infrastructures in unexpected situations. The ability to adapt and react to unforeseen events is taken into account.

These evaluation criteria not only identify the essential sectors within a state, ensuring the lives of citizens and the functioning of state systems, but also foresee the possibility that certain sectors may become critical in special situations. Through this approach, the development of potential security risks is quickly anticipated, thus strengthening the approach to their prevention and management.

With these in mind, we aim to present those essential sectors and services within which critical infrastructures operate, as they have been defined in the national legislative framework. In this sense, at the level of the Romanian state, they were officially established by GEO 98/2010, in which Annex no. 1 which are those sectors identified as having within them critical infrastructures for the security of the state, which we have illustrated in *figure 1*.



The energy sector

ICT sector

Water, forest and environment sector

Food and agriculture sector

The health sector

The cultural and heritage sector

The national security sector

The administration sector

Transport sector

The industrial sector

Space and research sector

Financial banking sector

Figure no. 1. Key sectors (OUG 98/2010)

Thus, these sectors were officially designated as essential sectors. As we can see, they all represent systems and infrastructures that support the existence of modern states with a contemporary lifestyle, thus being essential to maintain the current standard of living and functionality of the states.

The energy sector takes the first place in the list, for good reasons: ensuring energy security is not only a necessity, but also an essential condition for the efficient operation of all other critical infrastructures. Both real and virtual infrastructures, as well as every citizen, depend on the existence and proper functioning of infrastructures within the energy sector. Electricity is essential to society, making this sector vital to the functioning of a state. Nowadays, energy security and protecting its critical infrastructures is becoming a matter of national security, especially as energy consumption is growing exponentially. Energy production is carried out through various critical infrastructure systems, such as thermal, nuclear, wind or solar.

On the other hand, **the information and communication technology (ICT) sector** is booming, capturing global attention. Large organizations, regardless of their goals, and states currently rely on critical infrastructure consisting of physical or virtual networks and systems that use ICT technologies. This sector has evolved rapidly following technological advances in recent decades, driven by the emergence and development of computer systems capable of performing highly complex tasks. With IT technology becoming accessible to anyone with average resources to purchase a computer, the systemic risks of critical ICT infrastructures have increased significantly.

The water, forest and environment sector is included in the list of vital sectors for a fundamental reason: the environment, which includes both the biosphere and inanimate elements, represents the essential physical framework in which all infrastructures must exist in order to function properly. Its importance is not only limited to the support of critical infrastructures, but the specific environmental problems of the 21st century, generated by phenomena related to global warming, can represent significant threats to their operation. Extreme weather events such as storms, hurricanes or earthquakes can disrupt the operation of critical infrastructures, potentially causing major disasters. A conclusive example of this is the impact of a tsunami on critical energy infrastructure in Japan, in the case of the Fukushima incident. The nuclear power plant exploded due to the tsunami, endangering not only regional energy security, but also the health and physical integrity of citizens. Thus, meteorological phenomena can become real threats to critical infrastructures, and the general functioning of the environment directly influences people's quality of life. Within this sector, special attention is also paid to issues related to the supply of drinking water, considered a fundamental element for the existence and support of life.

The food and agriculture sector is in direct connection with the environment and is designated as an essential sector due to its direct role in producing the means necessary for human survival. With the population explosion beginning in the 19th and 20th centuries, the pressure on the agricultural and food sectors increased significantly as the ever-increasing number of people was able to outstrip the food production capacity. This situation can lead to a food crisis, where food security becomes a major problem. Within this sector, food supply chains are of crucial importance. A relevant example is observed in the context of the war in Ukraine, where the disruption of the export chains of wheat and other agricultural products in this country generated not only the increase in food prices, but also critical food crisis situations. This highlights the fragility and interdependence of food supply chains and underlines the importance of proper management of this vital sector.

The health sector is a modern and developed component, although concerns for maintaining and sustaining human health have existed since immemorial times. The critical infrastructure in this system is made up of hospitals, treatment centers, and medical emergency management infrastructure. In the modern era, this sector has seen significant progress with the advancement of medical knowledge, leading to the gradual increase in people's life expectancy.

In developed countries, this life expectancy has exceeded 80 years, and in some cases even reached or exceeded 85 years. Modern means of combating disease and maintaining health are indispensable, especially in the context of demographic growth, because the larger the population of a state, the greater the demand on the medical infrastructure. This request and the associated challenges became evident during the 2020-2021 pandemic caused by the SARS-CoV-2 virus. The pandemic has highlighted the need to strengthen medical infrastructure and adequate resources to effectively manage emergencies of such magnitude.

The national security sector represents a component closely related to the issue of state security. Essential for the maintenance of state order and security, this sector becomes crucial in ensuring an optimal environment for the conduct of the lives of the citizens of that state. Security itself is considered a public good, provided by the state through law and order structures. Ensuring security can involve various modalities, and this vital sector faces numerous challenges related to maintaining and protecting modern states in the face of threats that can affect the physical integrity of their citizens. The mission of the national security sector becomes crucial in the context of the various challenges faced by modern states, whether they originate from external or internal threats. Protecting citizens and territory thus becomes a strategic priority for ensuring national stability and prosperity.

The administration sector includes all state institutions that have the responsibility to administer internal processes, with the aim of ensuring the provision of essential services and managing the budget obtained from taxpayers' contributions for the support and development of the state. Essential for creating an enabling framework and for the efficient management of natural and other types of resources in a territory, the administration sector plays a vital role in the macroeconomic functioning of a state. Within this sector, the critical nature derives mainly from the direct influence on citizens' rights and freedoms and how these are reflected in the provision of public administrative services. The efficient administration of this sector is essential for ensuring transparency, effectiveness and accountability in governance, having a direct impact on the quality of life and the participation of citizens in the decision-making and administrative process of the state. (Pătrașcu, 2022)

The transport sector is a vital part not only in the context of Romania, but also at the international level. The physical infrastructure of roads and other transport facilities is an essential component in the global and national economy, facilitating the efficient movement of goods and people. These infrastructures are fundamental to the conduct of trade between states, creating efficient supply chains that help reduce costs for various products and support modern lifestyles by globally redistributing various goods and facilitating communication between people.

The industrial sector represents one of the backbones of modern states, contributing significantly to the shaping of today's society. Following the industrial revolution, the automation of work processes and the use of machines allowed the development of large-scale production of goods, stimulating economic and technological progress. Its crucial role is to ensure the efficient use of natural and human resources in the territory managed by the state.

The space and research sector is an emerging branch, currently focused on research and innovations for the use of space resources, with the objective of their future substitution for terrestrial resources. Scientific research plays an essential role in all areas of knowledge, including the resilience and protection of critical infrastructures.

The financial-banking sector is considered vital for Romania, providing the necessary structure for the existence of the modern economy. The circulation of goods, services and works is possible through monetary exchanges, and this financial flow is largely optimized through increasingly electronic banking transactions. This sector also facilitates significant funding that supports development and innovation, thus essential for a modern state.

The cultural and heritage sector, the last mentioned in the list in GEO 98/2010, is particularly important, given that it refers to the elements that contribute to national identity. Culture, anchored in a territorial, historical and linguistic context, together with representative traditions and customs, constitutes one of the defining elements for the formation of modern states. By managing and maintaining this sector, the continuity of an essential purpose of the state's existence is ensured.

For the identification of a critical infrastructure within the previously listed sectors, there is a 4-stage procedure established at the legislative level, these stages being the following (OUG 98/2010):

- Stage no. 1 – Implementation of criteria and critical thresholds depending on the sector – critical thresholds are established that allow distinguishing between ordinary and critical infrastructures. These thresholds serve as identification tools for determining the critical nature of an infrastructure.
- Stage no. 2 – Evaluation of the infrastructure by applying the definition of a critical infrastructure according to the provisions of GEO 98/2010. In this stage, the infrastructure is analyzed and evaluated according to the parameters established in the normative act, determining whether it meets the specific criteria to be considered a critical infrastructure.
- Stage no. 3 – Application of cross-sectoral criteria and thresholds, which are not specifically related to the sector in which an infrastructure was initially identified as potentially critical. In this phase, aspects that transcend the specific domains are considered and contribute to the global assessment of the criticality of the infrastructure.
- Stage no. 4 – Formulation of proposals for the designation of the infrastructure that has reached this stage as a national critical infrastructure. Based on the results of the sector-specific and cross-sectoral assessments, reasoned proposals are developed for the official designation of infrastructure as critical at national level.

The process of identifying and designating critical national infrastructures is a complex one, but it can be summarized in a logical scheme, also reflected in the legislation in force. This process is rigorously regulated, with the aim of ensuring that the infrastructures identified as critical are truly vital to the security of the state and the maintenance of modern living standards. Special attention is paid to avoiding the unnecessary waste of resources to infrastructures incorrectly considered critical, resources that could be more effectively redirected to sectors with real needs.

On the other hand, the absence of a well-defined process could lead to the possibility of not identifying some critical infrastructures, an unfavorable situation that would expose these infrastructures to major security risks. In the absence of an organized approach, there is a threat that these critical infrastructures will not benefit from the appropriate level of protection, leaving them vulnerable to the exploitation of their potential vulnerabilities.

At the level of the Romanian state, there are clear regulations in the field of the protection of critical infrastructures, including the specification of the essential sectors within which such infrastructures are found. Knowledge of these sectors is essential so as to understand how the processes of identification and protection of critical infrastructures are organized in Romania, and implicitly, in the European space. This regulated approach contributes to strengthening national security and ensuring effective protection of vital infrastructures for the functioning of the state and society.

BIBLIOGRAPHY:

1. Alexandrescu, Grigore, Văduva, Gheorghe, *Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție*, Editura Universității Naționale de Apărare „Carol I”, București, 2006;
2. Badea, Dorel, *Protecția infrastructurilor critice – structuri și funcționalități integratoare,* Editura Academiei Forțelor Terestre „Nicolae Bălcescu”, Sibiu, 2015;
3. Cîrdei, Ionuț Alin, *Aspecte privind protecția și reziliența infrastructurilor critice,* Editura Academiei Forțelor Terestre „Nicolae Bălcescu”, Sibiu, 2019;
4. Pătrașcu, Petrișor, Nicoară, Gabriela, *Public administration and critical infrastructure protection*, în „Anales Universitatis Apulensis – Series Jurisprudentia”, nr. 25/2022;
5. Rizea, Marian, Marinică, Mariana, Barbăsură, Alexandru, Dumitrache, Lucian, Ene, Cătălin, *Protecția infrastructurilor critice în spațiul euroatlantic*, Editura Ani, București, 2008;
6. H.G. 1110/2010 privind componența, atribuțiile și modul de organizare ale Grupului de lucru interinstituțional pentru protecția infrastructurilor critice;
7. H.G. 35/2019 pentru desemnarea autorităților publice responsabile în domeniul protecției infrastructurilor critice naționale și europene;
8. H.G. 718/2011 pentru aprobarea Strategiei naţionale privind protecţia infrastructurilor critice;
9. O.U.G. nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice.

1053477-3045-1396-24-47

THE ROLE OF CRITICAL INFRASTRUCTURE IN ENSURING SUPPLY CHAIN RESILIENCE

Simona Cristiana UNGUREANU
Second lieutenant, "Carol I" National Defense University, Bucharest, Romania
E-mail: simonaungureanu0740@gmail.com

Abstract*: The economic resilience of critical infrastructures is essential in an era of increasing interconnection and dependency. This article explores the complex field of critical infrastructure, highlighting both its vulnerability to numerous threats and its essential role in the functioning of modern civilisation. Focusing on the idea of economic resilience, we examine how resilient critical infrastructure is to disruptions and how quickly it recovers to minimise negative economic impacts.*

Keywords*: economic resilience, critical infrastructures, interconnection, vulnerability, threats.*

Introduction

Critical infrastructure and supply chains are two vital components of our modern economy and society. Critical infrastructure includes essential systems and services such as electricity, drinking water, transport, communications and financial systems that support the normal functioning of our society. Supply chains, on the other hand, are complex and interconnected networks of producers, suppliers, transporters and distributors that ensure the flow of goods and services from producers to consumers.

In a world characterized by rapid change and diverse threats, ensuring the resilience of these two entities is particularly important. Resilience refers to the ability of a system or organization to cope with and adapt to disruptions, whether natural or man-made. In the context of critical infrastructure and supply chains, resilience means the ability to prevent, recover from and minimize the impact of unexpected events or disruptions to these vital systems.

The aim of this essay is to explore and analyze the crucial role that critical infrastructure plays in ensuring supply chain resilience. It will examine how critical infrastructure and supply chains are interconnected, highlighting the importance of a robust critical infrastructure in ensuring effective functioning and supply chain resilience in the face of increasingly complex challenges.

In the following lines, we will take a closer look at the key concepts underlying this essay, such as 'critical infrastructure', 'supply chain' and 'resilience', to gain a deeper understanding of their interaction and importance in the current global context.

Defining key concepts

Critical Infrastructure

Critical infrastructure refers to a wide range of networks and systems that are essential to the functioning of the economy and modern society. Although the term 'critical infrastructure' has different meanings in different domains and geographies, industries such as electricity, water, transport, telecommunications and financial services are commonly included (Cybersecurity and Infrastructure Security Agency - CISA, 2020). Because of their interdependencies, these systems are susceptible to cascading effects from disruptions in another sector (Fîță, Radu et al. 2021, 36-57). Assessing economic resilience requires an understanding of these links.

Critical infrastructure is the group of systems, facilities and services that are essential to the functioning of a country's society and economy. These include, but are not limited to, electricity, natural gas, water and sewage networks, transportation (highways, railways, ports, airports), communications (telephony, internet, television), financial and healthcare systems, and other critical elements that support our daily lives (Fîță, Nicolae, 2020). Critical infrastructure is particularly important because the malfunction or disruption of these systems can have serious consequences for society and the economy.

One of the key characteristics of critical infrastructure is its interconnection with other sectors and industries, including supply chains. For example, companies depend on transport networks and logistics infrastructure to deliver products to their destinations. Freight transport also requires energy supply, communications management and access to financial services. Therefore, any disruption in critical infrastructure can have a direct impact on supply chains, affecting the supply of goods and services to consumers and businesses. (Baltasiu, Radu, 2011)

Supply chain

A supply chain is a complex network of organizations, processes and resources that work together to deliver goods and services from producers to consumers (Felea, Albăstroiu, 2013). This chain includes producers, suppliers, transporters, distributors and, in the end, final customers. Supply chains can range from simple to very complex, depending on the industry and the product or service provided.

A crucial aspect of supply chains is their interdependence. A disruption in one part of the chain can affect the whole system. For example, in the event of a disruption in the supply of materials or components, production can be affected, which can lead to delays in the delivery of products to customers. Therefore, supply chain resilience involves not only effective risk management, but also the ability to quickly adapt the chain to cope with changes or disruptions (Bucovețchi, Diana, 2020, 180-201).

Resilience

Resilience refers to the ability of a system or organization to adapt to disruptions, to recover quickly and to maintain essential functioning in the face of these disruptions. This concept applies to both critical infrastructure and supply chains (Bănică, Alexandru, Ionel, 2015). In the context of critical infrastructure, resilience implies the ability to prevent or minimize disruptions, effectively manage crises and ensure the essential functioning of systems even under difficult conditions. For example, a resilient electricity network can cope with extreme weather conditions or other events that could cause power outages.

Measuring and improving economic resilience in critical infrastructure is a challenging task. To assess resilience, researchers have developed a variety of frameworks and approaches, such as qualitative assessments, simulation tools and quantitative models, these methods consider variables including resource allocation, adaptability and redundancy as important indicators of resilience (Maupeou, Stanislas, 2009).

The need to increase infrastructure resilience has also been recognized by international governmental bodies and organizations. Through risk management, information sharing and coordinated response activities, programmes such as the US National Infrastructure Protection Plan (NIPP) aim to improve the security and resilience of critical systems.

In terms of supply chains, resilience means the ability to cope with disruptions, quickly adapt transport routes or sources of supply, and maintain the delivery of goods and services to customers. For example, in the event of disruption at a crucial import port, a resilient company can quickly find alternatives to avoid disrupting the supply of materials (Fîță, Nicolae, Dragoș, et. al., 2022).

These key concepts - critical infrastructure, supply chain and resilience - are closely related and form the basis for analysing the role of critical infrastructure in ensuring supply chain resilience. Next, we explore how these concepts interact and translate into practice within our modern economy and society.

Supply Chain vulnerabilities

Many risks and vulnerabilities affect critical infrastructure. Natural disasters, including hurricanes, earthquakes and floods, have the potential to cause significant damage and interfere with the provision of vital services. With the ability to compromise data integrity and interfere with operations, cyber-attacks have become a major concern (Alvarez et al., 2021). Infrastructure resilience is further challenged by the long-term effects of climate change, which include sea level rise and extreme weather events.

Supply chains, while essential to the economy, are exposed to a variety of vulnerabilities that can affect their normal functioning. These vulnerabilities can be grouped into several important categories, and in this segment of the essay we will focus on some of the most significant ones:

Dependence on globalization

Modern supply chains have become increasingly global, with production and distribution expanding internationally. While this globalization can bring economic benefits and efficiency, it can also create significant vulnerabilities. Reliance on production and sourcing from foreign countries can expose supply chains to geopolitical risks, sudden changes in trade policies or logistical disruptions such as Suez Canal blockages or disruptions in international transport (Soldi, Giovanni, et. al. 2023).

Reduced or nonexistent storage

In the quest for efficiency, many companies have reduced their inventories to a minimum or even eliminated them entirely, adopting just-in-time strategies. This can cut costs, but makes supply chains vulnerable to disruption. A disruption in the supply of essential materials or components can have an immediate impact on production and deliveries, without the ability to rely on buffer stocks to cushion shocks. (FRUNZETI, TEODOR, 2010)

Climate and natural hazards

Supply chains are vulnerable to climate and natural hazards such as storms, earthquakes and floods. These events can damage infrastructure, disrupt transport and affect production capacities. For example, an earthquake in a key production region or major port can lead to significant disruptions in supply chains ("Joint Communication to the European Parliament and the Council." A strategic approach to resilience in EU external action, 2017).

Technological vulnerabilities

The use of technology in supply chains can create vulnerabilities to cyber-attacks or technical failures. A security breach in a company's IT systems can lead to data loss or shut down operations. Also, dependence on technology can make supply chains vulnerable to disruptions in the supply of electronic components or software problems.

Social risks

Social protests, strikes or pandemics can affect supply chains by disrupting work or blocking transport. The COVID-19 pandemic, for example, had a significant impact on production and deliveries worldwide, highlighting social and human vulnerabilities in supply chains (Fîță, Nicolae, Sorin, et. al., 2021).

These vulnerabilities are just some of the challenges facing supply chains in modern society. It is important to understand these risks and take action to manage and minimize their impact. In the following part of the article, we focus on the role of critical infrastructure in addressing these vulnerabilities and ensuring supply chain resilience.

The Importance of Critical Infrastructure in the Supply Chain

Critical infrastructure plays a vital role in ensuring the efficient functioning and resilience of the supply chain in a world of complexity and uncertainty. This importance stems from the tight interconnection between critical infrastructure and supply chain processes, which affect every aspect of our economy and our daily lives.

First and foremost, critical infrastructure provides the essential resources needed for the supply chain to function (ARION, Stelian, Critical infrastructure protection - security management at owner and operator level (Critical infrastructure protection - security management at the level of owners and operators, 2018). For example, we can mention electricity grids power factories and logistics centers, ensuring the operation of machinery and equipment needed for production and distribution. Drinking water and sewage systems are vital for hygiene and production processes. Communications are needed for efficient coordination of transport and real-time information exchange within supply chains.

Secondly, critical infrastructure provides logistics and transport support, which are key elements in supply chains. Ports, railways, airports and motorway networks facilitate the movement of goods to and from factories, warehouses and distribution points. An efficient transport network is essential for delivering products to customers on time and keeping transport costs competitive. (Cavelty, Suter, 2012)

In addition, critical infrastructure helps to manage and minimize risks associated with supply chain vulnerabilities. Through investments in cyber security, climate and natural risk management, and emergency planning and preparedness measures, critical infrastructure can help prevent or reduce the impact of supply chain disruptions (Fridbertsson, Njall, 2023).

In conclusion, critical infrastructure is inherently linked to the functioning of supply chains and their resilience. Without a robust and reliable critical infrastructure, supply chains would be unable to deliver essential goods and services in an efficient and secure manner. Thus, the importance of critical infrastructure in ensuring the functioning and resilience of supply chains cannot be underestimated, and investment and risk management measures are crucial to sustain these vital systems.

Case studies and Practical examples

To illustrate the impact and importance of critical infrastructure in ensuring supply chain resilience, we will focus on two significant case studies and practical examples that have demonstrated the connection between these two key elements.

Case study 1: Cyber-attacks on electricity grids in Ukraine

In December 2015 and 2016, Ukraine witnessed cyber-attacks on its electricity networks. These attacks resulted in the disruption of electricity supply in large regions, affecting both domestic consumers and local industries. The case study highlights how vulnerable critical infrastructures can be to cyber-attacks and the importance of cyber security in ensuring the functioning of supply chains, especially in key sectors such as electricity. (The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict, 2023)

Case study 2: The COVID-19 pandemic and global supply chains

The COVID-19 pandemic, which broke out globally in 2020, has highlighted vulnerabilities in global supply chains. In the context of this pandemic, companies have faced disruptions in the supply of components and raw materials, the closure of production facilities and major disruptions in transportation. The case study reveals the direct impact on supply chains and the need to develop resilience strategies that take into account risks such as pandemics in supply chain planning and management. (Moosavi J, Fathollahi-Fard AM, Dulebenets MA. Supply chain disruption during the COVID-19 pandemic: Recognizing potential disruption management strategies. Int J Disaster Risk Reduct, National library of Medicine (COVID-19 and its impact on the global supply chain – A short review, 2021).

Practical example: Amazon's transport and storage system

Amazon, one of the world's largest online retailers, is a prime example of critical supply chain infrastructure. The company has developed an extensive network of distribution centers, warehousing facilities and transportation systems to deliver products to customers globally. The ability to keep this critical infrastructure functioning is crucial to ensuring Amazon's supply chain resilience and customer satisfaction (Bucovețchi, Diana, 2018).

These case studies and practical example demonstrate that critical infrastructure plays a critical role in sustaining supply chains and protecting their resilience. They highlight the importance of proper management and investment in critical infrastructure to avoid and minimize the impact of disruptions to supply chains and to ensure the continued supply of goods and services in modern society.

Improvement Measures and Solutions

To strengthen the resilience of supply chains and ensure their effective functioning in the face of identified vulnerabilities, there are many measures and solutions that organizations, governments and industry as a whole can adopt. (ARION, Stelian, 2011).

- Diversification of supply sources: Reducing dependence on critical suppliers or regions by diversifying supply sources can minimize the impact of disruptions. To this end, companies can evaluate and develop relationships with alternative suppliers or consider domestic production for certain components or products;
- Strategic stocks: Reviewing stock management strategies to include strategic reserves in case of emergency can help cushion the impact of disruptions and keep the supply chain functioning during crises;
- Advanced monitoring and technology: Investing in advanced supply chain monitoring and tracking technologies can help identify and respond quickly to problems or disruptions. Sensors, blockchain technology and data analytics can provide real-time visibility into supply chains;
- Business continuity plans: developing and implementing business continuity plans, which include procedures and protocols for managing crises and maintaining essential operations during disruptions, are essential;
- Collaboration and communication: Cooperation between organizations, governments and other stakeholders on risk management and crisis response is crucial. Sharing information

and best practices can contribute to better preparedness and more effective emergency management; (Lukitsch, Muller, Stahlhut, 2018)

- Investing in critical infrastructure: Governments should continue to invest in upgrading and protecting critical infrastructure, including cyber security, to reduce vulnerabilities and ensure resilience to threats;
- Education and training: Developing a workforce prepared and trained for risk management and crisis response is essential to ensure resilience (Felea, Albăstroiu, 2013).

Ultimately, the implementation of these measures and solutions must be tailored to the specific needs of each organization and be part of a proactive approach to ensuring supply chain resilience in the face of a changing environment and increasingly complex risks.

Evaluation of Efficiency and Benefits

Assessing the effectiveness of measures and solutions implemented to strengthen resilience supply chains and critical infrastructure is essential to measure their impact and benefits. In this assessment, the following aspects should be taken into account: (Bănică, Alexandru, Ionel, 2015)

- Increased resilience: A key indicator of efficiency is the ability of the supply chain to cope with disruptions and recover quickly. Reducing downtime and minimizing losses can be measured to assess the effectiveness of implemented solutions;
- Reduced costs: If the measures have helped reduce the costs of disruptions and interruptions in the supply chain, this can be an indication of the financial benefits of the investment;
- Improved cyber security: For cybersecurity-related solutions, reduced security incidents and breaches can be measured, as well as the ability to prevent or limit the impact of cyber-attacks;
- Operational efficiency: Improvements in supply chain management, as well as increased efficiency and visibility, can contribute to an overall increase in operational efficiency; (Fîță, Nicolae, Sorin, et. al., 2021)
- Risk mitigation: benefit assessment should also include an analysis of reduced or more effectively managed risks, such as climate, geopolitical and technological risks;
- Reputation and trust: Increasing the trust of customers and business partners can be another measure of effectiveness, as it can help strengthen business relationships and enhance the organization's reputation.

We can conclude that in a world characterized by disruption and uncertainty, where supply chains and critical infrastructure play a vital role in providing the goods and services we need for our lives, the importance of building resilience cannot be underestimated. This essay has explored the role of critical infrastructure in ensuring supply chain resilience and highlighted the close connections between these two key elements.

Identified vulnerabilities in supply chains, such as excessive globalization, low inventories or dependence on technology, are real challenges facing organizations and society as a whole. However, by implementing appropriate measures and solutions, such as diversification of supply sources, inventory management and investment in cyber security, the resilience of supply chains and critical infrastructure can be strengthened.

Evaluation of the effectiveness of these measures shows that investments in resilience can bring significant benefits, including increased resilience, reduced costs and improved security. However, it is important to continue efforts to strengthen resilience, as threats and risks can evolve over time.

Thus, managing risks and ensuring resilience in supply chains and critical infrastructure is imperative to address contemporary challenges and ensure the continued delivery of goods and services for the benefit of society. Through collaboration, appropriate investment and taking a proactive approach, we can help create a more resilient and secure future for all.

BIBLIOGRAPHY:

1. Bănică, Alexandru, and Ionel Muntele. Resilience and territory - conceptual operationalization and methodological perspectives. Iași: Terra Nostra Publishing House.
2. European Commission. 2017. "Joint Communication to the European Parliament and the Council." A strategic approach to resilience in EU external action. http://www.cdep.ro/eu/examinare_pck.fisa_examinare?eid=528.
3. Fîță, Daniel Nicolae, Mihai Sorin Radu and Dragoș Păsculescu. 2021. Energy security assurance, control and stability in the context of increasing industrial and national security. Petroșani: Universitas Publishing House.
4. Fîță, Nicolae Daniel. 2020. Research on the identification of vulnerabilities of critical infrastructures within the National Ultra and Very High Voltage Electricity System with international connection. PhD thesis. Petroșani: University of Petroșani.-. 2019. Identification of vulnerabilities of critical infrastructures within the National Electric Power System in the context of increasing energy security. Petroșani: Universitas Publishing House.
5. Fîță, Nicolae Daniel, Dragoș Păsculescu, Cristina Pupăză and Emilia Grigorie. 2022. "Methodology for the identification, designation, analysis, assessment, protection and resilience of critical power infrastructures." In Resilience Management in Contemporary Society, by Olga Maria Cristina
6. Bucovețchi (coordinators) Diana Elena Ranf. Sibiu: Nicolae Bălcescu Academy of Land Forces Publishing House.
7. Fîță, Nicolae Daniel, Sorin Mihai Radu, Dragoș Păsculescu, and Emilia Grigorie. 2021. "Addressing national critical energy infrastructures correlated to societal resilience and sustainability." In Sustainability management and managerial sustainability between classical and modern paradigms, by Olga Maria Cristina Bucovețchi, Dorel Badea (coordinators) Diana Elena Ranf, 37-58. Sibiu: Nicolae Bălcescu Academy of Land Forces Publishing House.
8. ARION, Stelian, Critical infrastructure protection - security management at the level of owners and operators (www.revista-alarma.ro)
9. Translated with www.DeepL.com/Translator (free version)Felea, Mihai; Albăstroiu, Irina (2013) : Defining the Concept of Supply Chain Management and its Relevance to Romanian Academics and Practitioners, Amfiteatru Economic Journal, ISSN 2247-9104, The Bucharest University of Economic Studies, Bucharest, Vol. 15, Iss. 33;
10. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf
11. Moosavi J, Fathollahi-Fard AM, Dulebenets MA. Supply chain disruption during the COVID-19 pandemic: Recognizing potential disruption management strategies. Int J Disaster Risk Reduct, National library of Medicine (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9027543/)
12. Cybersecurity and Infrastructure Security Agency - CISA, 2020
13. Baltasiu, Radu. 2011. "Lecture Notes." Master in Security Studies II - Societal Risks and Cyberspace.
14. De Maupeou, Stanislas. 2009. "Internet, nouvelle infrastructure vitale!" Revista Défense nationale et sécurité collective.

15. Soldi, Giovanni, et. al. 2023. "Monitoring of Underwater Critical Infrastructures: the Nord Stream and Other Recent Case Studies." Electrical Engineering and Systems Science (Cornell University)
16. Fridbertsson, Njall T. 2023. Protecting Critical Maritime Infrastrcture - the Role of Technology. General Report, NATO Parliamentary Assembly, NATO Parliamentary Assembly.
17. Lukitsch Kristof, Muller Marcel and Stahlhut Chris, Criticality in Jens Ivo Engels, Key Concepts for Critical Infrastructure Research, Springer VS, Weisbaden, 2018
18. Cavelty Myriam Dunn and Suter Manuel, The Art of CIIP Strategy: Tacking Stock of Content and Processes in Lopez Javier, Setola Roberto, Critical Infrastructure Protection: Information Infrastructure Models, Analysis and Defence, Springer, Heidelberg, 2012
19. Frunzeti, Teodor, Protection of critical infrastructure - priority task within the security strategy of the European Union, Military Sciences Review, 2010

1053477-3045-1396-24-48

NEW DIMENSIONS OF CRITICAL INFRASTRUCTURE PROTECTION – OFFSHORE CRITICAL ENERGY INFRASTRUCTURES

Alexandru GEORGESCU, PhD.
Industrial Engineering, National Institute for Research and Development
in Informatics ICI Bucharest, Romania
E-mail: alexandru.georgescu@ici.ro

Maria-Mihaela GURĂU, PhD
International Relations and European Studies, Euro-Atlantic Resilience Centre, expert,
Bucharest, Romania
E-mail: maria.gurau@e-arc.ro

***Abstract**: The Critical Infrastructure Protection paradigm is in wide use among Western allies and partners. It has registered continuous development as more critical infrastructure domains and more interdependencies are brought to light by the effects of the "perma-crisis" affecting the world in the recent years. The article highlights the issues surrounding the offshore critical infrastructure, and specifically analyzes critical energy infrastructures in a European context. These systems feature unique requirements and challenges, not just in terms of their functioning, but also for their security governance. Given the normalization of hybrid warfare against civilian critical infrastructures, as well as expected development in offshore critical energy infrastructures, national security and defense decision and policy makers must develop a better understanding of these systems.*

***Keywords:** offshore critical infrastructure, energy infrastructure, resilience, cyber, maritime domain.*

Introduction

Critical Infrastructure Protection (CIP) is a framework in use at the level of the EU, the US and elsewhere that offers the concepts and tools to perform a systemic analysis of the wider society, both within national borders and beyond it, in order to identify and designate the critical infrastructures (CI) on which we depend for our social, political and economic lives (Gheorghe et al, 2018). CI produce critical goods and services as well as facilitate the normal functioning of society and they include roads, ports, pipelines, power plants, but also financial markets, public administration, hospitals, and labs. Every entity performing CIP creates its own taxonomy of CI, based on its understanding of the field, but they generally include sectors such as energy, agriculture and food, transport, chemical industry, health and more (Georgescu & Bucovetchi, 2023). Infrastructures can generally be defined as socio-technical systems made up of key assets, resources, organizations, and functioning frameworks; to be critical, their destruction or disruption would have to cause significant loss of human life, material damages and loss of confidence. CIP acknowledges that we cannot protect all the critical infrastructures all the time, and provides the methodologies and the critical thresholds to identify the truly critical infrastructures in order to concentrate scarce security resources and attention span on improving their security outcomes, by regulating their functioning, establishing a partnership with the owner/operator (often a private company) and by promoting their resilience (Georgescu & Bucovetchi, 2023).

CIP is a framework-program at both national and European levels. The former concerns the national perspective and has wide variation, the latter ensures minimum standards overall for EU Member States and relates to the European Critical Infrastructures (ECI) whose disruption or destruction affects two or more MS or, in the case of ECI of particular European significance according to the recently adopted Critical Entities Resilience Directive, affects six or more MS.

The recent events have revealed what the World Economic Forum has termed both perma-crisis and poly-crisis, partly as a result of global interdependencies, tight couplings between global systems ensuring the propagation of risks and disruptions, and problems with global security governance. Perma-crisis reflects the succession of crisis events that have continuously affected the EU since the late 2000s, starting with the 2008 Global Financial Crisis, then the European sovereign debt crisis, the refugee crisis, the Covid-19 pandemic and then the Russian invasion of Ukraine (Tharoor, 2023). All of these crises have happened in the backdrop of rapid technological change, volatility in key market sectors such as energy and other factors which put pressure on the ability of society to handle such issues and to recover. This is referred to as a poly-crisis, in which crisis events or at least stressors are seen in various fields, such as finance, energy, food, physical security (Torkington, 2023).

They feed off each-other in vicious cycles, challenging the capacity of the authorities and various other stakeholders to properly address them because of their self-escalating or cascading natures (Pescaroli & Alexander, 2016). These phenomena underscore the multisector and multidisciplinary approaches required to perform security governance in the current environment, while also pointing the difficulties encountered by the authorities which act within properly delineated jurisdictions (such as state borders) or within discrete sectors (energy, civil defense, health).

The perma- and poly-crisis situations have led to gradual changes in the European and EU Member States' (MS) governance frameworks for CIP. In particular, new sectors of CI have been identified at national levels (such as financial infrastructure and cultural patrimony in 2018 in Romania), but especially at European levels, where the 2022 CER Directive (European Parliament, 2022), due to be transposed by EU MS into national legislation by 17 October 2024, has identified 11 CI sectors for ECI identification and designation (energy, transport, banking, financial market infrastructure, digital infrastructure, health, drinking water, wastewater, public administration, space and production, processing, and distribution of food), in contrast to the two sectors that had previously been the case (energy and transport). Additionally, it must be mentioned that this Directive complements the NIS 2 Directive.

This article concerns itself with the issue of Offshore Critical Infrastructures (OCI), which the Nord Stream 1 and 2 sabotage and other incidents have demonstrated as posing unique challenges for security governance stakeholders. The use of hybrid warfare by countries such as Russia but also China against OCI has underscored the coercive potential of OCI targeting, whether in a conventional or asymmetric conflict. In particular, we will look at Offshore Critical Energy Infrastructures (OCEI), which could be described as an emerging weak point for an EU which is trying to expand OCEI to promote energy independence and energy resilience while encountering unique challenges to CI resilience.

Chapter 1 Offshore Critical Infrastructures

OCI are systems which are partly or completely located in a maritime environment. If we employ on a system-of-systems perspective, we find that CI can have other CI as components making up a wider system-of-systems that produces critical goods or services (Katina and Keating, 2015). Therefore, OCI can be viewed as standalone infrastructures, as components of larger maritime infrastructures, or as components of mixed land-sea-air-space infrastructures. These are often critical, given the expense of creating and maintaining them, which is justified only for infrastructures which account for high levels of utility to their respective countries, and given the potential side-effects of their disruption or destruction, which can include severe environmental damage or the cascading disruptions of other CI chains, such as those in global transport and logistics, or in energy. OCI can either be on the water surface or underwater. While not offshore in a literal sense, the shore infrastructures, located where the maritime and land domains meet and providing the critical transition space, often with a technical role, should also be considered an OCI, since they share many of them same specific characteristics and issues with governance.

OCI include the maritime components for a wide range of critical infrastructures, including but not limited to energy, transport, communications, but also food (through fisheries and also global food distribution chains) or national security and defense (through maritime surveillance).

Table 1 presents some key issues distinguishing them from other land-based infrastructures, in a generic sense.

Table no. 1: Characteristics of Offshore Critical Infrastructures

Characteristic	Explanation
Hostile environment	Infrastructure that is partially or completely submerged in water can experience various forms of degradation, especially in saltwater, high humidity or exposed to saltwater sprays. The presence of storms and other adverse weather effects, including the kinetic damage from impact with waves, requires ruggedized infrastructure systems. Spontaneous malfunctions are possible.
Difficulty in repair, maintenance, replacement	Compared to the generic terrestrial infrastructures, OCI are more difficult to access for repairs, maintenance, and replacement, which can also take place in more difficult conditions. It is also possible that, like certain land CI, OCI operate continuously and at high levels of total capacity, with minimal operational margins, making unplanned interventions both difficult and potentially disruptive in the context of continuous functioning.
Difficult surveillance and monitoring	Compared to land CI, OCI operate in poorly surveilled environments, with gaps in coverage by sensors or by Earth Observation systems, with varying levels of environmental awareness possible, including in the degree of mapping of the undersea relief, or in the understanding of complex weather phenomena and water currents.
International environments	Depending on which maritime environment we are discussing, it is possible that the OCI operates partially or completely in international waters or in exclusive economic zones, where there is lower surveillance capability and where potential threat actors can engage in various destabilizing or disruptive actions. The level of acceptance of the international framework governing activities at sea is neither universally recognized, nor complete in terms of setting out precise terms governing harmful events, attribution, and response, especially given the variety of OCI.
Additional operational constraints	The OCI operators also face concerns regarding the potential impact of disruptions on issues other than their functioning and that of their dependent entities. Concerns regarding the environmental damage of spills and the uncertainties of penalties and other forms of punishment for such occurrences generate an additional level of uncertainty that can modify stakeholder behavior and influence the governance framework.

Chapter 2: Offshore Critical Energy Infrastructures

OCEI are a particular form of OCI that is of interest given their variety, their geopolitical importance, and their criticality to European security of supply. The EU and its partners are important operators of OCEI and current plans envision a growing inventory of European OCEI in the future, responding to requirements for greater interconnectivity, greater offshore renewable generation and greater oil and gas extraction (at least in the short and medium term).

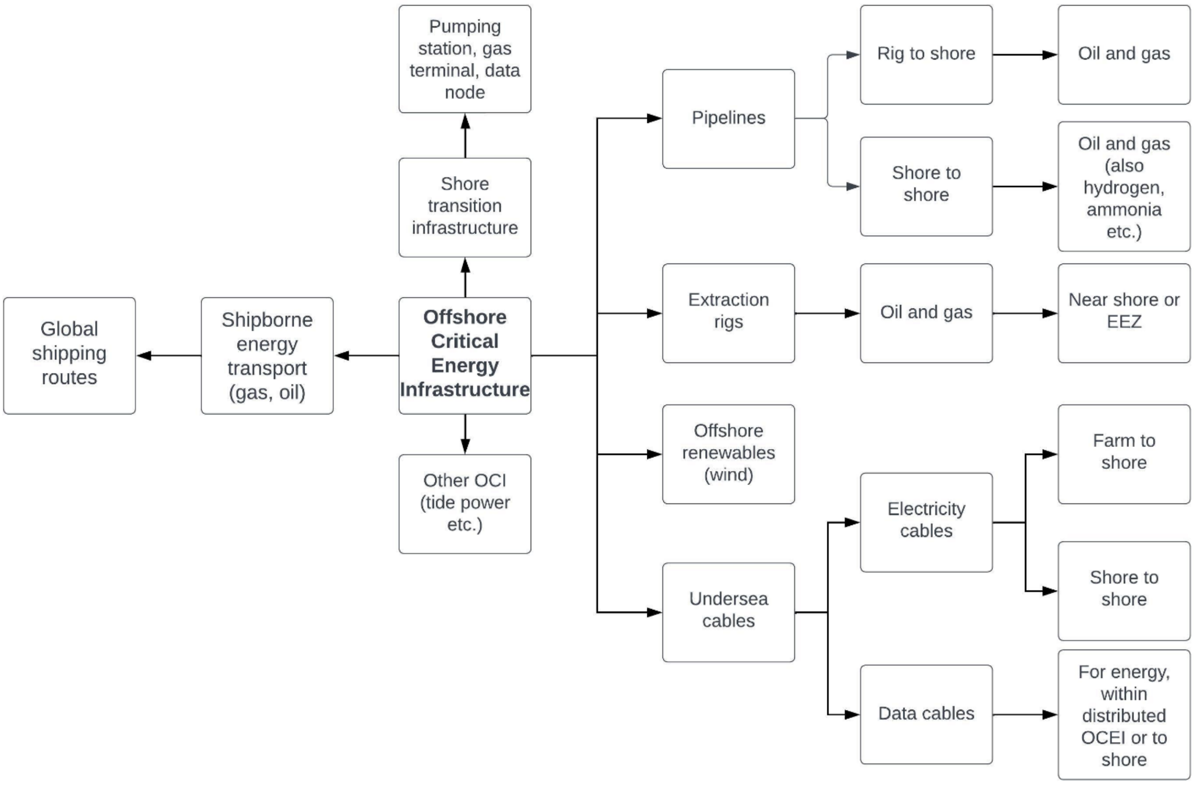

Global shipping routes
Shipborne energy transport (gas, oil)
Offshore Critical Energy Infrastructure
Pumping station, gas terminal, data node
Shore transition infrastructure
Other OCI (tide power etc.)
Pipelines
Extraction rigs
Offshore renewables (wind)
Undersea cables
Rig to shore
Shore to shore
Oil and gas
Oil and gas
Oil and gas (also hydrogen, ammonia etc.)
Near shore or EEZ
Electricity cables
Data cables
Farm to shore
Shore to shore
For energy, within distributed OCEI or to shore

Figure no. 1. Main types of Offshore Critical Energy Infrastructures
Source: authors

OCEI have come into the public consciousness through the Nord Stream 1 and 2 pipeline sabotage, which was both difficult to investigate and took place under conditions of low surveillance capacity, especially underwater, and high levels of international tensions (given the Russian invasion of Ukraine). At the time of the writing of this article, there still were no results of the investigation into the sabotage.

Other incidents include the cutting of the fiber optics cables connecting Norway to its satellite communication center on the island of Svalbard (Humpert, 2022) and the cutting (and disappearance) of 4,3 km of undersea cable from a maritime surveillance network in the North Sea which also resulted in the disappearance of ten tons of cable (Kulha, 2021).

Combined with observations of an ostensibly civilian Russian ship with armed crew members appearing to map the undersea cables, speculating to be rehearsing the sabotage of undersea OCI (Bueger et al, 2022), there has been a surge of interest in our ability to understand and protect OCEI given that it has become a target for hybrid warfare. Although these are civilian systems, we have witnessed the normalization of threats and attempted disruptions of Critical Energy Infrastructures (CEI) as a result of the geopolitical pressures surrounding the Russian war in Ukraine. While it is obvious why a country like Russia would target Ukrainian CEI, given that it is vital for the operation of society and of the Armed Forces and therefore can be used to degrade capabilities, interrupt normal operations in the economy and coerce the population and the leadership, we have seen hybrid attacks also against the CEI of other countries. Attacks featuring attribution challenges, such as cyber attacks especially but also drone attacks, cable cutting and other forms of sabotage are also practiced by countries that can maintain deniability or maintain the effects of their gray zone operations beneath the threshold of armed response from the victim (Bueger et al, 2022).

They can be used to degrade capabilities or put pressure on the economy through market reactions, but also to threaten and discourage involvement and to reduce confidence in the country's leadership for failing to protect society from such inevitably high profile disruptions. In the case of maritime territorial disputes between China and other countries, we have seen harassment of oil rigs, including ramming, as a way to assert ownership of a disputed area, to discourage private operators from using the site and to escalate conflict.

Chapter 3: Characteristics of OCEI and their security environment

As can be seen from figure 1, OCEI are very diverse and consequently feature a very different array of issues, especially in a European context, where different regions have different OCEI. We can state that they have the following characteristics, in addition to the ones of OCI in general:

- Growing reliance on digitalized and networked systems, especially for active system management;
- Attractive and highly visible target of attack, if only to temporarily disrupt rather than destroy;
- Increasingly unmanned or undermanned, relying even for maintenance checks on unmanned systems;
- Undergoing a boom driven by ideological considerations regarding decarbonization, energy independence, security of supply, gas as a transition fossil fuel, and the very high interest in offshore renewables.

3.1. Energy extractions rigs

These include the large oil rigs which extract oil and gas from offshore deposits and send them to shore either by ship or by pipelines. Figure 2 shows the distribution of EU oil and gas installations according to the 2021 EU data (European Commission, 2023b).

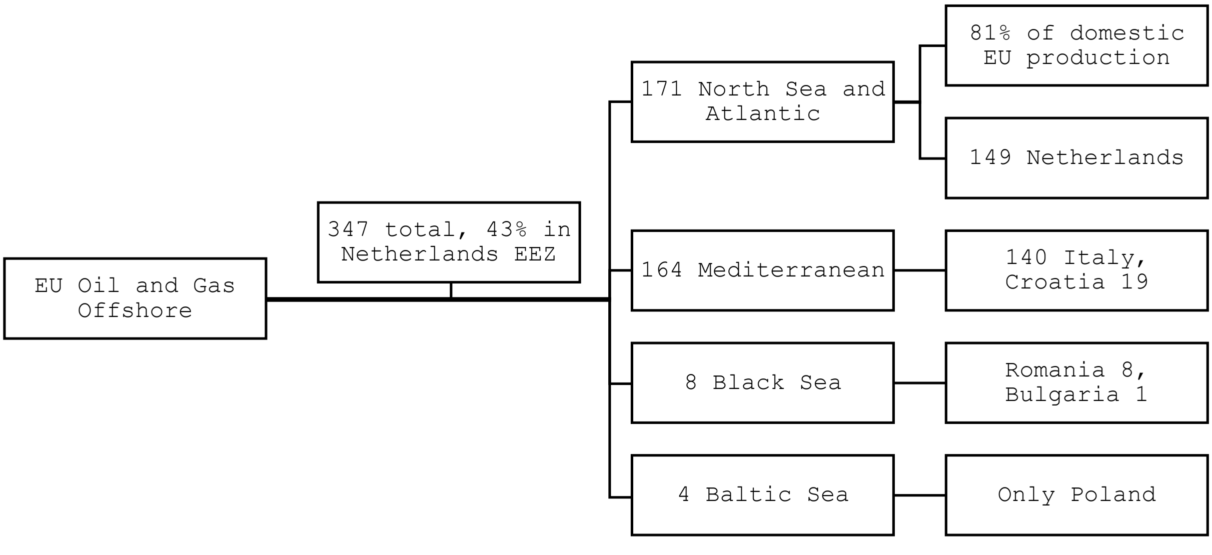


Figure no. 2. Offshore oil and gas installations in the EU, 2021 data (European Commission, 2023b)

Offshore oil and gas in the EU produce 14,710 kilotonnes of oil equivalent (ktoe), which is 70% gas and 30% oil by volume (European Commission, 2023b). The Netherlands is the undisputed champion of offshore oil and gas in the EU, though the UK was a strong second before Brexit. However, Romania is planning on becoming a stronger extractor of Black Sea gas, especially given the Netherlands' decision to wind down extraction and conserve its reserves.

Directive 2013/30/EU provides the main framework for EU offshore oil and gas intallations, which it defines as "a stationary, fixed or mobile facility, or a combination of facilities permanently inter-connected by bridges or other structures, used for offshore oil and gas operations or in connection with such operations. Installations include mobile offshore drilling units only when they are stationed in offshore waters for drilling, production or other activities associated with offshore oil and gas operations" (European Parliament, 2013). It features connected, "within the safety zone or within a nearby zone of a greater distance from the installation at the discretion of the Member State: (a) any well and associated structures, supplementary units and devices connected to the installation; (b) any apparatus or works on or fixed to the main structure of the installation; (c) any attached pipeline apparatus or works" (European Parliament and Council, 2013).

3.2. Pipelines

Pipelines provide continuous transmission of fossil fuels (and, potentially, other substances such as a hydrogen mix) either between two shore installations connecting national pipeline grids or between offshore oil and gas installations and a landing area (potentially with storage or continuing land pipelines) or a central processing location which relies on tankers for transmission to shore.

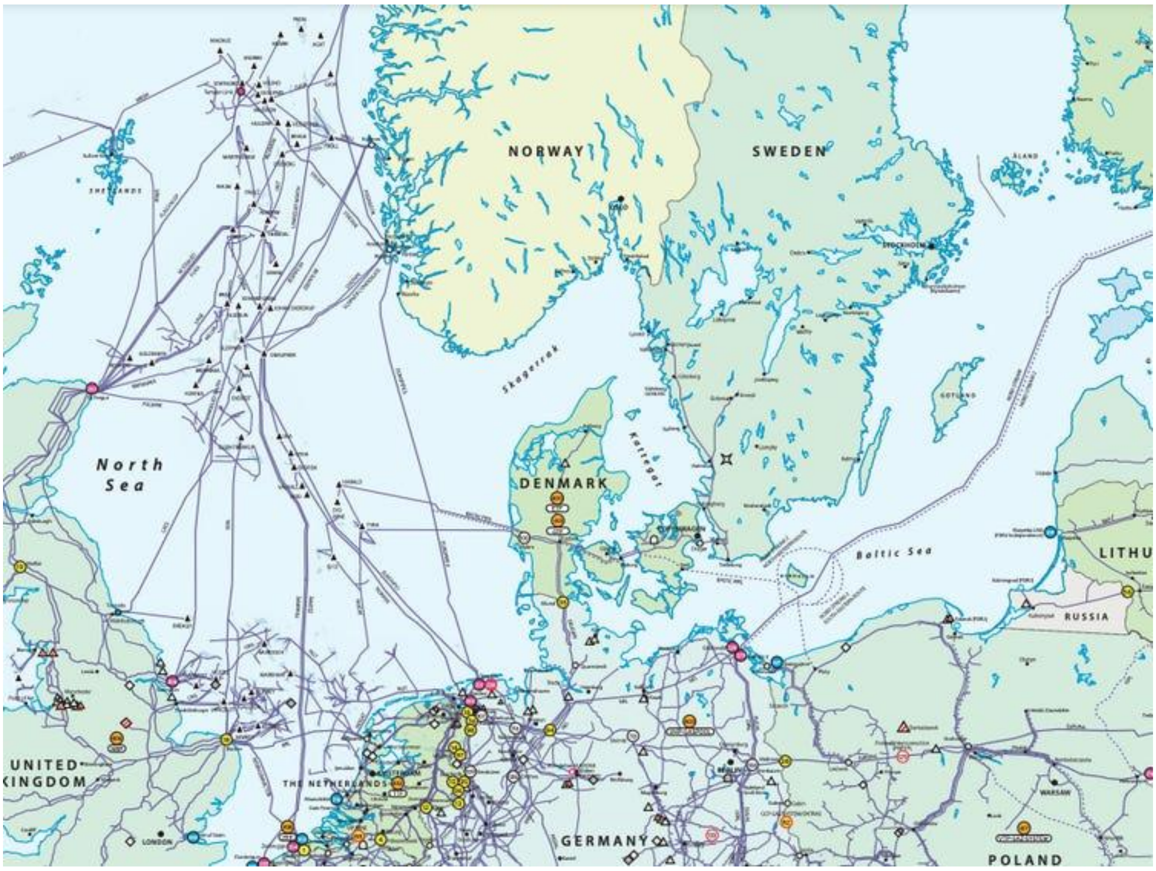


Figure no. 3. Map of oil and gas pipelines offshore in Northern Europe (Hogg, 2022)

Figure 3 shows a map of pipelines in the North Sea and the Baltic Sea, no including the recent gas pipelines connecting Norway to Poland. Directive 2013/30/EU states that the EU recognizes a difference between shore to shore pipelines connecting countries and the connecting infrastructures of oil and gas installations – “within the safety zone or within a nearby zone of a greater distance from the installation at the discretion of the Member State: (a) any well and associated structures, supplementary units and devices connected to the installation; (b) any apparatus or works on or fixed to the main structure of the installation; (c) any attached pipeline apparatus or works” (European Parliament, 2013). Pipelines can be damaged not just intentionally, but also as a result of natural factors including seismic activity, as well as various accidents. The European Parliament (2013) recognized that deliberate sabotage can be done either by ship, by underwater vessels, by a mix of these or by the use of unmanned vehicles including submersible drones.

3.3. Undersea cables

These are an “invisible” infrastructure connecting European countries to each other, to their neighbors and to other OCEI (Bueger & Edmunds, 2023). Globally, communication cables are responsible for 95% of communication capacity, with a large number of them being located in the water surrounding the EU and signs that non-state or state sponsored actors have begun targeting them, such as the recent news about the Houthis in Yemen disrupting cables under the Red Sea.

Undersea electricity cables, both on the sea floor and buried beneath it, have been an important part of electricity grids since the first high voltage line was inaugurated in 1954 in EU territory between the Swedish mainland and Gotland Island. They can act as cross-border interconnectors, enabling exchanges between two or more countries, or they can be laid out in arrays to connect the growing number of offshore wind farms (and potentially other renewables electricity sources like tide power stations or floating solar or even floating nuclear power) to the shore transmission station. In addition to existing electricity transmission cables, there are numerous projects planned, such as a new Netherlands-UK connector, a Greece-Egypt interconnector, and others.

Communication cables are also important in order to coordinate unmanned OCEI such as the individual elements of a wind farm.

Undersea cables can experience damage or destruction due to natural phenomena like rock slides creating abrasions, corrosion, seismic activity, or various currents. They can also be affected accidentally by human activity, such as getting caught in anchors, dredging devices or fishing gear. This is why there are even “cable awareness efforts” in very highly navigated waters such as between the UK and the Netherlands (figure 4).

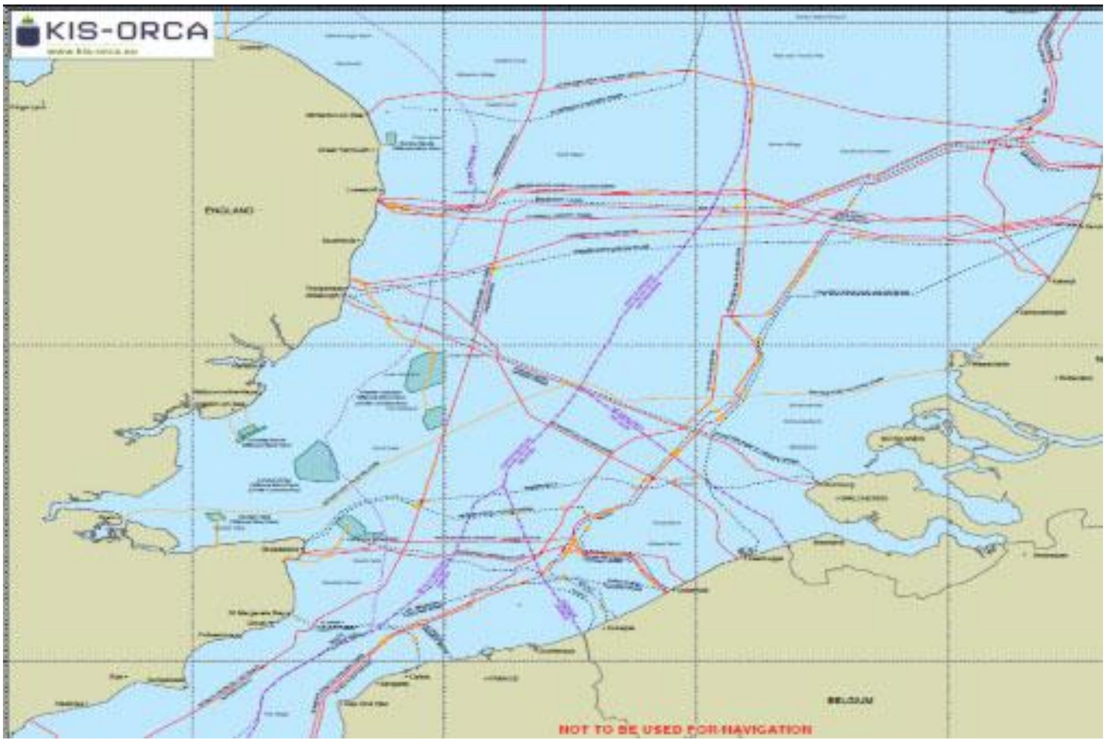


Figure no. 4. Chart showing all cable inter-connectors, export cables and telecommunications cables (ESCA, 2024)

Lastly, we have the deliberate threats, such as the aforementioned Russian activity (Bueger et al, 2022). There is, as of yet, no confirmed electricity cable that was cut deliberately, since there is an escalation risk involved, and 70% of incidents of severed cables in the last 30 years are confirmed to be of natural or accidental causes (Tang et al, 2021). Their growing numbers suggest that it is only a matter of time until a threat actor decides to use either sophisticated or more easily accessible means to sever electricity cables in order to disrupt the EU's interconnected Energy Union.

3.4. Offshore wind farms

Offshore wind farms are a very fast growing segment of the European renewable energy sector, allowing countries to utilize previously untapped wind potential. The largest concentration of offshore wind farms is in the Netherlands, where the first commercial offshore wind farm opened in 1991. Many more countries have built these systems and we are at the beginning of a new expansion phase (figure 5) permitted both by framework developments in countries such as Romania (which plans to have its first offshore wind farms by 2027-2028) and by technological development such as the floating wind turbines which can be placed much farther offshore with lower costs because they do not need to be tethered to the seafloor. They do, however, require active stabilization using cyber-physical systems, which are susceptible to cyber-attacks and other forms of interference. Concerns regarding the security of communications and electricity cables tying wind farms together and then to the shore infrastructure still apply.

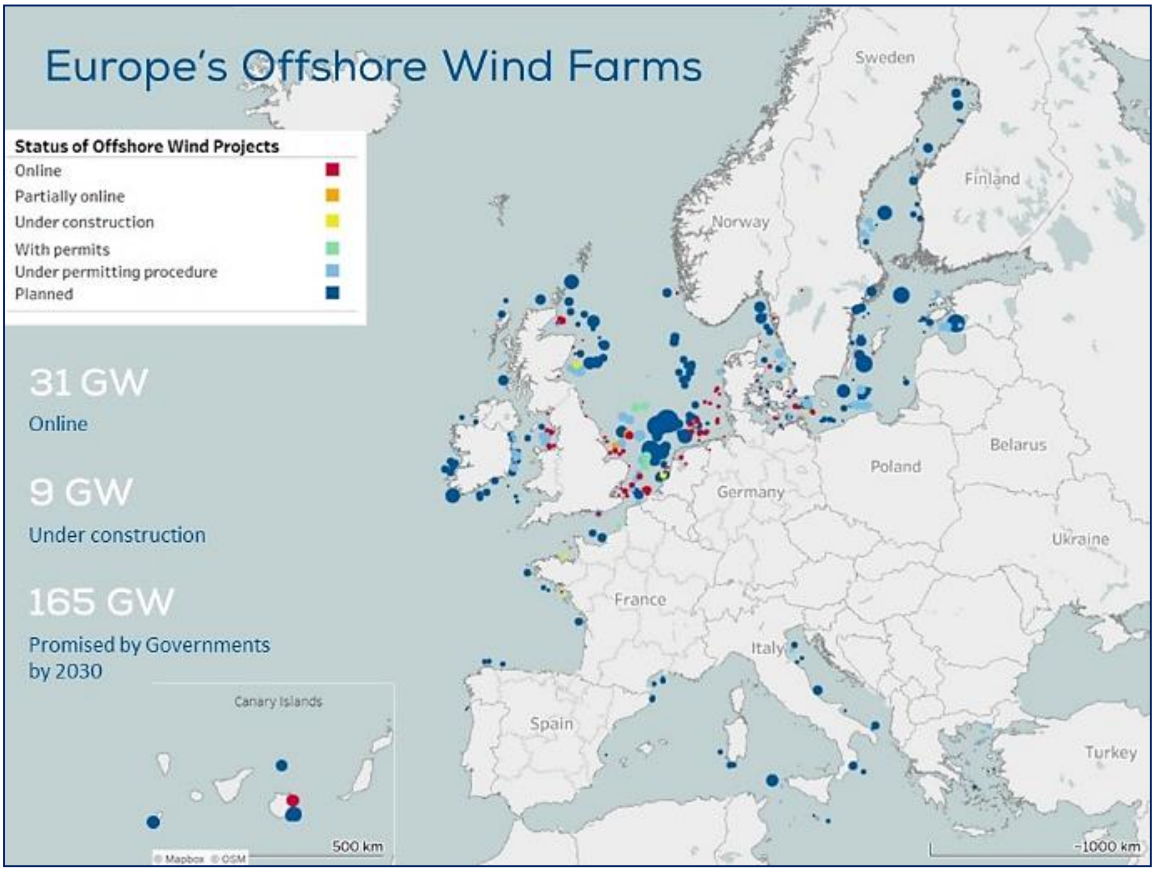


Figure no. 5: Wind farm map of Europe (WindEurope, 2024)

Offshore wind farms also illustrate some key points regarding the new generation of OCEI. Firstly, they have vulnerable supply chains, both in the need for Rare Earth Metals for the manufacturing of the turbines themselves, but also in the supply chain for specialized hardware and software that enables this OCEI to function. We may see more and more cyber attacks against the suppliers of specialized products and services to these OCEI, trying to take advantage of continuing contacts for software updates, for instance. It is also the case that, with digitalization, developers are using open-source libraries and other high performance and widely spread software for maximum capability and efficiency. This poses an additional risk (though it diminishes others), since hackers are more likely to be proficient in the particular operating systems, programming languages and the software of individual systems than they would have otherwise been.

Conclusions

Offshore Critical Infrastructure are an important subset of the CI which make globalization possible. They enable the flow of data, goods, and energy to all parts of the world. Offshore Critical Energy Infrastructures are a particular type of OCI characterized by high variety and a challenging security environment, enhanced, in the case of the EU, by the war in Ukraine, and also by developments such as new technologies, rapid expansion to increase energy independence from Russia and rapid expansion to meet decarbonization and internal energy production goals. The EU is highly exposed to threats affecting OCEI and its resilience requires a thorough understanding of OCEI, their uniquely challenging environment and their specificities. In this article, we laid the groundwork for the development of a systemic view on OCEI which can then be employed to analyze the effectiveness of security governance framework in the EU and to formulate recommendations to security policy makers and decision makers.

BIBLIOGRAPHY:

1. Bueger, C., Edmunds, T. (2023). The European Union's Quest to Become a Global Maritime-Security Provider. Naval War College Review. Vol. 76: No. 2, Article 6, 1-20
2. Bueger, C., Liebetrau, T., Franken, J. (2022). Security threats to undersea communications cables and infrastructure – consequences for the EU. European Parliament, Directorate General for External Policies of the Union. PE 702.557. https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2022)702557
3. European Commission (2023b). Report from the Commission. Annual Report on the Safety of Offshore Oil and Gas Operations in the European Union for the Year 2021. Brussels, 12.5.2023. COM(2023) 247 final
4. European Parliament (2013). Directive 2013/13/30/EU of the European Parliament and of the Council of 12 June 2013 on safety of offshore oil and gas operations and amending Directive 2004/35/EC. OJ L 178, 28.6.2013
5. European Parliament (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, published on 27.12.2022.
6. European Parliament (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, published on 27.12.2022.
7. European Submarine Cable Association (2024). Presentation page on submarine cables. As ESCA (2024), https://www.escaeu.org/articles/submarine-power-cables/
8. Georgescu, A., Bucovețchi, O. (2023). Protecția Infrastructurilor Critice – abordări conceptuale. Curs Universitar, Editura SITECH, ISBN 978-606-11-8547-4, Craiova, România
9. Gheorghe, A., Vamanu, D.V., Katina, P., Pulfer, R., 2018. Critical Infrastructures, Key Resources, Key Assets: Risk, Vulnerability, Resilience, Fragility, and Perception Governance, Topics in Safety, Risk, Reliability and Quality. Springer International Publishing. https://doi.org/10.1007/978-3-319-69224-1
10. Hogg, R. (2023). The security of Europe's oil and gas pipelines is at risk after the suspected Nord Stream sabotage. Here's a map of the sprawling network. Business Insider, 30 September 2022, https://www.businessinsider.com/take-look-europes-oil-and-gas-network-nord-stream-leaks-2022-9
11. Humpert, M. (2022). Nord Stream Pipeline Sabotage Mirrors Svalbard Cable Incident. High North News, 29 Sept 2022, https://www.highnorthnews.com/en/nord-stream-pipeline-sabotage-mirrors-svalbard-cable-incident
12. Katina, P. F., Keating, C. B. (2015) Critical infrastructures: A perspective from systems of systems. International Journal of Critical Infrastructures. 11(4). p.316–344.
13. Kulha, S. (2021). 4.3 Kilometers of Subsea Cable Vanished Off North Norwegian Coast. The Drive, 11 November 2021, https://nationalpost.com/news/world/norways-strategic-underwater-research-observatory-has-cables-cut-removed-in-suspicious-act
14. Pescaroli, G., Alexander, D. (2016). Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. Nat Hazards 82, 175–192. https://doi.org/10.1007/s11069-016-2186-3
15. Tang, W., Flynn, D., Robu, V. (2021). Sensing Technologies and Artificial Intelligence for Subsea Power Cable Asset Management. IEEE International Conference on Prognostics and Health Management (ICPHM). DOI: 10.1109/ICPHM51084.2021.9486586

16. Tharoor, I. (2023). The worry in Davos: Globalization is under siege. Washington Post, 17 Jan 2023, https://www.washingtonpost.com/world/2023/01/17/davos-globalization-wef-economic-seige/
17. Torkington, S. (2023). We're on the brink of a 'polycrisis' – how worried should we be? World Economic Forum, 13 Jan 2023, https://www.weforum.org/agenda/2023/01/polycrisis-global-risks-report-cost-of-living/
18. WindEurope (2024). Wind Energy Fact Sheets. https://windeurope.org/wp-content/uploads/images/about-wind/fact-sheets/

INDEX OF AUTHORS