"CAROL I" NATIONAL DEFENCE UNIVERSITY
(Highly appreciated publishing house within "Military science, intelligence and public order"
of Titles, Diploma and University Certificates Awards National Council)

ISSN 2668-1994
ISSN-L 2668-1994

PROCEEDINGS

Volume XVI, Part 2

"CAROL I" NATIONAL DEFENCE UNIVERSITY
SECURITY AND DEFENCE FACULTY

PROCEEDINGS

THE 16TH INTERNATIONAL SCIENTIFIC CONFERENCE
"STRATEGIES XXI"

STRATEGIC CHANGES IN SECURITY AND INTERNATIONAL RELATIONS

April 09-10, 2020

Scientific Editors:

Brigadier General Dorin Corneliu PLEŞCAN

Colonel Professor Ion PURICEL, PhD

Colonel Professor Daniel GHIBA, PhD

Colonel Professor Lucian Dragoş POPESCU, PhD

Colonel Professor Ioana ENACHE, PhD

Lieutenant-Colonel Professor Tudorel LEHACI, PhD

ProQuest

Volume XVI,
Part 2

"CAROL I" NATIONAL DEFENCE UNIVERSITY

SECURITY AND DEFENCE FACULTY

PROCEEDINGS

THE 16TH INTERNATIONAL SCIENTIFIC CONFERENCE "STRATEGIES XXI"

STRATEGIC CHANGES IN SECURITY AND INTERNATIONAL RELATIONS

Volume XVI, Part 2

Scientific Editors:

Brigadier General Dorin Corneliu PLEȘCAN
Colonel Professor Ion PURICEL, PhD
Colonel Professor Daniel GHIBA, PhD
Colonel Professor Lucian Dragoș POPESCU, PhD
Colonel Professor Ioana ENACHE, PhD
Lieutenant-Colonel Professor Tudorel LEHACI, PhD

April 09 - 10, 2020
Bucharest, Romania

INTERNATIONAL SCIENTIFIC CONFERENCE STRATEGIES XXI
"Carol I" National Defence University
Bucharest, Romania, April 09 - 10, 2020

Desktop publishing: Liliana ILIE
Cover designer: Andreea Elena GÎRTONEA

ISSN 2668-1994 (print); ISSN 2668-2001 (online)
ISSN-L 2668-1994

FOREWORD’

The papers reunited in the present volume have been submitted to The Sixteenth International Scientific Conference “Strategies XXI – Strategic Changes in Security and International Relations”, planned to be hosted by National Defence University “Carol I” in Bucharest, Romania, 09-10 April 2020.

Throughout the last year, the transformations in international relationships, the security challenges and crises emerging in almost all areas around the world, have demonstrated that predictability is still an illusion. The recent events in the entire world, not only in the Eastern and Southern regions of Europe have proven that detailed analyses are needed in order to reveal the impact of those challenges on strategic relationships.

Increasing the importance of artificial intelligence, the nonproliferation policy, the spread of terrorist acts, the tense transatlantic relation, the Syrian crises and the Turkish actions, the tensions in the eastern part of Europe as well as in the proximity of the Black Sea and the Mediterranean Sea areas, and last but not the list, the global scale COVID-19 Pandemy, are just a few of the security challenges that the states from the region and also the international and regional organizations are dealing with. All this spectrum of threats, especially its synergic effect, influences dramatically the entire human existence and is playing a substantial role in reshaping both global, regional and national security policies and strategies; that is why there are many questions regarding the way the international community should respond to these kinds of threats. Already formulated questions: „Should credibility of conventional deterrence and collective defence be rebuilt in the light of Russian new policy and its subsequent hybrid strategy?, or Crisis management operations should be the key to the future type of operations, and in that case should EU and NATO efforts improve their capabilities in that direction?” remains, and new others just rise from now on: Considering the current global scale Covid-19 Pandemy, is it the national or regional crisis management the proper, efficient and effective answer, or should be a global approach the correct answer for such challenge we are facing now and we will face, surely, in the next couple of years?”

In the future it is certain that the societies will be even more interconnected than they are today, continuing, either to benefit from globalization, either to loose due to no understanding its trends. The interaction between great powers, the less economically developed states, and non-state actors will achieve new dimensions, cyber attacks and sponsoring the terrorism will be new ways of exerting influence. Yet today terrorism, asymmetric and hybrid threats, health and environmental challenges, economic volatility, climate changes and energy insecurity endanger our people and the entire globe.

The center of gravity of global economic power is continuing to shift between Euro-Atlantic Region and Asia-Pacific Region, resulting a change in the balance of power and an increasingly inter-polar world. While the US is likely to remain the world leading military power, its military advantage is likely to be diminished and challenged increasingly by China and the Russian Federation. The BREXIT heavily contributed to the complexity of the situation. Hybrid activity is the enabler of repositioning on the global chess table. Rising powers, such as Brazil and India, will take a strategic interest beyond their own regions in pursuit of resources.

As the security of a nation should be the first duty of the state institutions, we should get deeply involved in finding solutions for promoting a sustainable peace and a more secure world, in using national capabilities to build prosperity and to use all the regional and international instruments of power to prevent conflicts and, when necessary, to engage the various spectrum of challenges in a comprehensive approach.

The new security challenges, supported by the overlapping processes such as globalization and fragmentation, combined with new concepts, forms and means of struggle for power and resources are added to the classic types of threats, risks and vulnerabilities generating crises. As nowadays situation proves, in case of inadequate answers, these new types of crises may evolve into a much shorter time, without geographical limitations, in all confrontation spaces and environments and *can quickly reach the stage of a total war, the highest manifestation of crises, a phase after which, most likely, all of us will have lost.*

The attempts to redefine the security environment have revealed the major factors that can influence the future of peace and security and at the same time they may be the cause of future violent conflicts. An inventory of possible characteristics of these factors highlights the change of their nature as well as their multiple forms of propagation. Due to the diverse, complex, interconnected, unpredictable and multidirectional character of the new threats, it becomes increasingly difficult to adopt and apply measures for crisis and conflict management.

In addition to the above, as the topics are becoming more consistent and gaining ground, more and more academic debates are taking place in the international relations and security areas, emerging both at the theoretical and practical level.

This year's Conference itself provides – as its organizing committee has stated – a forum for discussion on topics related to the security and international relations, military phenomena and related subject matters.

Taking into consideration that only a comprehensive international scientific effort won't prevent a conflict, but without it we cannot find the proper solutions, the mission of the International Conferences Strategies XXI is to facilitate communication between the international multidisciplinary teams.

The main areas of interest proposed for the submission of the papers cover the following sections:

- *Theoretical Aspects of Security and International Relations*
- *Processes and Phenomena of Globalization*
- *Defence Studies*
- *Military History, Geopolitics and Geostrategy*
- *Crisis Management and Conflict Prevention*
- *NATO and EU Policies and Strategies*
- *Humanitarian International Law*
- *Information Systems, Intelligence, and Cyber Security*
- *Public and Intercultural Communication and Social Security*
- *Defence Resource Management*
- *Education Sciences.*

The conference attracted over 97 papers but, in the end, after a very careful evaluation, only 73 (75,2%) papers were accepted. Considering 26 evaluators for the 11 up mentioned sections, there were 24 (24,8%) rejected papers, 16 (16,5%) papers accepted with amendments, and 57 (58,7%) papers accepted as such.

Finally, we would like to thank to all participants who shared their expertise with colleagues for this volume. We also hope that the papers included in this volume will give new ideas to the readers in their quest for solving various problems.

The publisher is honored to inform the authors and readers that the previous Proceedings of the International Scientific Conference "Strategies XXI – Strategic Changes in Security and International Relations" are indexed in the ProQuest Central database.

The conference would not have been possible without the joint effort of the organizing committee (Security and Defence Faculty / "Carol I" National Defence University) and the evaluating board, to whom we are deeply grateful.

Brigadier General Dorin Corneliu PLEȘCAN, Commandant (Rector),
"Carol I" National Defence University
Professor Daniel GHIBA, PhD, Vice-Dean for Scientific Research,
Security and Defence Faculty,
Associate Professor Cosmin OLARIU, PhD and
Lecturer Cristian ICHIMESCU, PhD, Conference Administrators,
Chairs of International Scientific Conference "Strategies XXI", 2020
"Carol I" National Defence University, Romania

CONTENTS

Crisis Management and Conflict Prevention

Chairs:

Iulian CHIFU, PhD
Ciprian IGNAT, PhD

FORMALIZED SCENARIO BUILDING ADAPTATION FOR CONFLICT PREVENTION

Adriana ILAVSKA
Researcher, Masaryk University, Czech Republic
424083@muni.cz

Martin CHOVANCIK, Ph.D.
Assistant Professor, Masaryk University, Czech Republic
chovancik@fss.muni.cz

Abstract: *Scenario-building methods are broadly employed to assist prediction and planning across a broad field of applications. Security environment analysis and conflict prevention planning has predominantly relied on long-term trend assessments by experts and infrequently on basic scenario building. The mode of scenario building was characterized by high-volume or extreme case methodology. The high number of possible scenarios and assignment of probabilities present key disadvantages. The paper proposes an adaptation of Trend Impact Analysis (TIA) methodology to security environment analysis and conflict prevention by illustrating this application on a dataset of 12 monitored trend factors specifically tested on a set of 316 cases. The application shows that TIA combines the advantages of quantitative and scenario-building methods to systematically reduce the number of probable scenarios and increase the precision of predictions necessary for effective analysis and conflict prevention. This application is highly relevant to both state and international medium and long-term conflict prevention and threat mitigation strategies.*

Keywords*: conflict prevention, scenario-building, trend impact analysis.*

Introduction

Prediction in social sciences and namely impactful security issues has always been a core challenge of security analysts, military planners, and political scientists. While a plethora of approaches have been applied, refined, adapted, discarded, and reinvented - the post-Cold War transformation of addressing conflict has established several dominant patterns. These are characterized by a rapid and profound transformation of peacekeeping and peace enforcement, but also quite significantly, a re-focus on conflict early warning, prediction, and prevention[1].

While conflict resolution approaches have been tested by fire throughout the 1990s and daily ever since, conflict prevention remains much more elusive and overlooked - but may also be quite effective and cheap. Its methods span from structural prevention programs such as UN Good Offices or the European neighborhood Policy, to sophisticated quantitative methods predicting hotspots with machine-learning[2], and stand-by mediation teams ready for deployment.

[1] Bredel, Ralf, *Long-term conflict prevention and industrial development: the United Nations and its specialized agency, UNIDO* (Leiden: Brill, c2003); Babbitt, Eileen F. "The Evolution of International Conflict Resolution: From Cold War to Peacebuilding," *Negotiation Journal* 25, no. 4 (October 1, 2009): 539–49, https://doi.org/10.1111/j.1571-9979.2009.00244.x; Gross, Eva.*EU conflict prevention and crisis management: roles, institutions, and policies* (London: Routledge, 2014); Zartman, I. William. *Preventing deadly conflict* (Malden, MA: Polity Press, 2015).

[2] Basuchoudhary, Atin, James T. Bang, Tinni Sen, and John David. *Predicting hotspots: using machine learning to understand civil conflict* (Lanham, Maryland: Lexington Books, 2018).

Whether considered an element of preventive diplomacy or pre-emptive diplomacy[3], most prolifically written about by Michael S. Lund in his many works, tools of conflict prevention are rapidly developing around the same core concepts - long-term peacebuilding efforts coupled with predictive methods to concentrate and intensify these efforts in specific times and locations. These methods are often less understood and even more frequently laborious and distrusted. If prediction and early warning serve as necessary identifiers of risk areas where violence is likely; scenario building offers the production of actionable probability assessments to address emanating threats.

Proactive engagement in early stages of conflict is necessary for both operational and structural prevention[4]. In an emerging crisis, fundamentals for early warning are provided by an analysis of structural causes and triggers. Identification of structural causes supports long-term structural prevention. On the other hand, operational prevention is based mostly on detecting proximate causes and triggers. Monitoring them enables faster reaction, crucial for containing escalation[5]. However, early warning is in itself inefficient in averting, containing, or mitigation and almost irrelevant to long-term planning of capacities within the observing country - despite significant progress in its methodology[6]. It is a base for creating targeted responses and guiding decision makers to take the best and most effective action under the time constraint[7]. Even in this regard Early warning systems are plagued by the curse of the "response gap": the actual follow-up of warnings by action[8].

In spite of the considerably long tradition of early warning and conflict predictions, both topics are still controversial in the field of conflict research[9]. N.N. Taleb identified several issues of human predictions and predictions in "soft" sciences. Besides the individual bias, one of the main problems of qualitative approach is overestimating predictions. Humans tend to exaggeratedly rely on their own estimations if they are based on a large amount of information[10]. To address this issue, the prediction process became more formalized and engaged quantitative methods. Firstly, traditional extrapolation techniques were introduced into predictions. Forecasting techniques became more sophisticated since the 1960s[11]. However the central issue of quantitative techniques could not be eliminated neither by improving computational power nor by enlarging used data sets. The problem lies in the main assumption of extrapolation, that the future will be similar to the past[12]. Therefore,

[3] Steven A. Zyck and Robert Muggah, "Preventive Diplomacy and Conflict Prevention: Obstacles and Opportunities," *Stability* 1, no. 1 (September 25, 2012): 68–75, https://doi.org/10.5334/sta.ac.

[4] Susanna Campbell and Patrick Meier, "Deciding to Prevent Violent Conflict: Early Warning and Decision-Making within the United Nations," 2007, 32, https://irevolution.files.wordpress.com/2011/07/campbell-meier-isa-2007.pdf.

[5] Herbert Wulf and Tobias Debiel. 2009. Conflict Early Warning and Response Mechanisms. A Comparative Study of the AU, ECOWAS, IGAD, ASEAN/ARF and PIF. no. Crisis States Working Papers Series No.2.

[6] Hegre, H., Karlsen, J., Nygård, H. M., Strand, H., & Urdal, H. 2013. Predicting Armed Conflict, 2010–20501. *International Studies Quarterly*, 57(2), 250–270. https://doi.org/10.1111/isqu.12007

[7] Claus Neukirch, "Early Warning and Early Action – Current Developments in OSCE Conflict Prevention Activities," 2013.

[8] Wulf, H., & Debiel, T. 2010. Systemic disconnects: Why regional organizations fail to use early warning and response mechanisms. *Global Governanc*e, 16(4), 525–547; Bock, J. G. 2014. Firmer Footing for a Policy of Early Intervention: Conflict Early Warning and Early Response Comes of Age. *Journal of Information Technology & Politics*, 12(1), 103–11; Rohwerder, B. 2015. *Conflict Early Warning and Early Response*. Governance Social Development Humanitarian Conflict Helpdesk Research Report, 13.

[9] Lars-Erik Cederman and Nils B. Weidmann, "Predicting Armed Conflict: Time to Adjust Our Expectations?," *Science*, no. 355 (2017): 474–76, https://doi.org/10.1126/science.aal4483.

[10] TALEB, Nassim Nicholas. *The black swan: the impact of the highly improbable* (London: Penguin, 2008)

[11] William R. Huss, "A Move toward Scenario Analysis," *International Journal of Forecasting*, 1988, https://doi.org/10.1016/0169-2070(88)90105-7.

[12] William R. Huss and Edward J. Honton, "Scenario Planning-What Style Should You Use?," *Long Range Planning*, 1987, https://doi.org/10.1016/0024-6301(87)90152-X.

extrapolation techniques can produce only surprise-free predictions. But our world, especially the world of security issues and conflicts, is definitely not surprise-free.

Jointly, the deficiencies of - early warning, the response gap, and surprise-free extrapolation techniques in forecasting - create the need for a methodology ascertaining the risk of said surprise and predicting the possible fallout of that surprise. In the field of security analysis and conflict prevention, the preferred method is scenario building.

Scenario building allows for planning out possible surprises in the trends as well as the necessary responses ahead of time. Compared to prediction and early warning, scenario building offers both - the alternative outcomes of a situation which we might then be alerted of by an early warning system, and the range of actions to follow these alternatives.

However, much like with forecasting - the determination of probabilities is fraught with deficiencies. What is more, to adequately cover a security issue, threat, or prediction of conflict impacts - dozens of scenarios have to be produced. The current method of minimization rests with expert consultations, worst case scenario building only, or other eleminitation methods to reduce the number of scenarios[13].

The proposed text offers an example of employing a tool not used in conflict prevention and threat mitigation scenario building - Trend Impact Analysis (TIA) in conjunction with Qualitative Comparative Analysis (QCA) - as a method of increased prediction preciseness and a method automatically assigning probabilities to scenarios. The obvious benefit to security analysis and conflict prevention being the reduced number of scenarios with already designated probabilities - focusing resources and conflict prevention capacities to the scenarios deemed most impactful in respective sectors. We introduce a real-world analysis of a small state's optimization of scenario building to rationalize resource dedication to highest impact scenarios in individual spheres - migration is used as an example, due to the ease of quantification, but the process is applicable to any defined threat possibly emanating from a conflict scenario.

Scenario-building approach: Trend Impact Analysis

Predictive analyses in the field of security or politics are still rare. It seems scepticism still prevails originating in the supposed inability of predicting social reality because of its overwhelming complexity[14]. A scenario-based approach to the future might be more acceptable even for sceptics because a scenario is not "a future reality but rather a means to represent it with the aim of clarifying present action in light of possible [...] futures."[15] It makes scenarios suitable for long-term evaluation of the future in uncertain environments characterized by lack of data and a considerable number of variables that are extremely difficult or impossible to quantify. Scenarios were introduced in the 1950s by Herman Kahn and even though their application is mainly in business, the initial application was related to military and strategic studies[16]. The first comprehensive model for scenario-building was

[13] Schwenker, Burkhard, and Torsten Wulf. *Scenario-Based Strategic Planning : Developing Strategies in an Uncertain World* (Munich: Springer Gabler, 2013) Martelli, Antonio. *Models of Scenario Building and Planning: Facing Uncertainty and Complexity* (New York: Palgrave, 2014).

[14] Kalous Miroslav, "Analysis of several pioneering studies in the field of Czech political and security scenario-building." *Obrana a Strategie*. 18(1):131 - 146. doi:10.3849/1802-7199.18.2018.01.131-146.

[15] Philippe Durance and Michel Godet, "Scenario Building: Uses and Abuses," *Technological Forecasting and Social Change*, 2010, p.1488 https://doi.org/10.1016/j.techfore.2010.06.007.

[16] William R. Huss, "A Move toward Scenario Analysis," *International Journal of Forecasting*, 1988, https://doi.org/10.1016/0169-2070(88)90105-7.

published in 1975[17] but it took almost another 3 decades for the use of the method to spread. Only in the last 15-20 years scenarios are on the upswing[18].

In the context of a gradual evolution of scenario-building, three main alternative approaches can be identified. The first category of techniques is based on intuitive logic, the second category is more formalized, and engages cross-impact analysis. The third category, trend impact analysis based scenarios, combines more traditional forecasting techniques with qualitative factors[19]**).** This is a desirable combination for predictions in security studies.

However, it is important to emphasize once again, scenarios are not forecasts. Their primary task is not to anticipate the future but they do promote thinking of the environment as a network of independent relationships rather than a cluster of variables. A scenario exercise is more a simulation than a forecast, it is a model which duplicates structure and actions of the environment[20]**.** It can be a huge advantage in combination with their strong narrativity because through scenarios using trend impact analysis, issues identified by formalized and precise methods can be translated into terms of the real world and become actionable. Intelligibility of results of scenario exercise in conflict prevention for all relevant actors in the process is the crucial factor for interconnecting long-term planning, early warning, and early and appropriate action.

Trend impact analysis seems to be the best candidate for meeting the goal of integrating forecasting into planning. The common practice of TIA application follows rules of traditional surprise-free extrapolation, combines them with inputs from qualitative methods and ties both together by narrative targeted to future actions. The very first step to final scenarios is identifying key scenario drivers for the chosen problem. By doing that, the researcher demarcates scenario space and can work with time series and trends in the defined space. So-called naive extrapolation follows. Variables and their trend is analyzed by traditional quantitative methods. After surprise-free extrapolation, the innovation of TIA transpires. The next step is introducing impacting events, there are a few ways to identify these events, i.e. literature review, experts' opinions, results of the Delphi method. When the set of events is assembled, every event must be specified in more detail. Namely, when will the event's impact on trend occur, how long will it take till the event causes the most significant shift in the trend, what is the highest possible impact and how long will it take until the shifted trend becomes a new standard. Equally important is to define the probability of every event and also probabilities of details on the event's development. With the specified scale of possible impact and probabilities, it is possible to revisit the original extrapolation and adjust it to different events. At this point, a single extrapolation breaks up into dozens of scenarios.

Unlike the other approaches to scenario-building, trend impact analysis assigns probability and impact to every scenario and significantly facilitates the process of choosing relevant options and developing narratives in particular scenarios[21].

From the method description, it is clear TIA offers a solution for many issues that need to be addressed to achieve the integration of forecasting into planning. Unquantifiable variables cannot be neglected and tools for the prediction cannot be indifferent to the unexpected turning points. Both points are addressed by integrating experts' opinions,

[17] George Wright, Ron Bradfield, and George Cairns, "Does the Intuitive Logics Method - and Its Recent Enhancements - Produce 'Effective' Scenarios?," *Technological Forecasting and Social Change*, 2013, https://doi.org/10.1016/j.techfore.2012.09.003.

[18] Martelli, *Models of Scenario Building and Planning: Facing Uncertainty and Complexity*.

[19] William R. Huss and Edward J. Honton, "Scenario Planning-What Style Should You Use?," *Long Range Planning*, 1987, https://doi.org/10.1016/0024-6301(87)90152-X.

[20] Martelli, *Models of Scenario Building and Planning: Facing Uncertainty and Complexity*.

[21] William R. Huss and Edward J. Honton, "Scenario Planning-What Style Should You Use?"; Martelli, *Models of Scenario Building and Planning: Facing Uncertainty and Complexity*.

literature reviews comprising mostly case studies, and taking into account possible twists in trends caused by unexpected events. Another important point for linking both aspects of successful conflict prevention and management is macro environment analysis and interconnection of long-term analysis and consideration of short-term changes[22]. TIA, which successfully covered previous issues, is not so strong in addressing the latter, however, in the conflict prevention macro environment it becomes crucial. Therefore we decided to modify TIA in a few steps to increase the chance it will comprehensively cover a broader environment and combine long-term and short-term factors.

Trend Impact Analysis adaptation: small state action in conflict prevention and threat mitigation - example of migration to Czechia

Small states are the ideal users of TIA in conflict prevention. With limited resources to conduct extensive assessments of threats through scenario building and equally limited resources to engage in threat impact mitigation and prioritization - TIA offers a rationalization of both types of resources. Exemplified by a threat of irregular migration, Czechia is utilized as a small state with limited capacities pro-actively seeking to improve its security in guarding against negative impacts of possible armed conflict in the proximate neighborhood. The impacting "surprise" therefore is established to be an armed conflict. Conflicts and especially civil wars are well-recognised drivers of forced migration[23] and for preventing forced migration it is important to focus on conflict prevention[24]. Irregular migration is identified by Czechia as a security risk it wishes to mitigate. A lot of attention is paid to migration as a factor increasing crime and causing the growth of the labor black market, but there is also an issue of cultural consequences. If it is combined with the rise of xenophobia and lack of integration, social cohesion can be endangered[25] and also stability of state institutions if the migration is massive and institutions are failing to manage it. Therefore it is necessary to monitor how migration evolves in time[26].

Regarding monitoring migration, countries usually have to focus primarily on geographically close regions. For European countries the potential threat can come from Europe itself, Middle East, North Africa, Central Asia, Caucasus, and Russia. Those countries should be regularly inspected and if an internal conflict, as a source of migration, may occur - preventive action to manage the conflict and attenuate possible consequences should be launched. For the case of the Czech Republic regions of interest remains the same, in three main groups - Western Europe, Post-Communist space, Middle East and North Africa - 86 individual countries will be included into analysis and inspected on possibility of conflict

[22] William R. Huss, "A Move toward Scenario Analysis."

[23] Christina Davenport, Will Moore, and Steven Poe, "Domestic Threats and Forced Migration, 1964-1989," *International Interactions* 29, no. 1 (2003): 27–55, https://doi.org/10.1080/03050620304597; Will H Moore and Stephen M Shellman, "Whither Will They Go? A Global Study of Refugees' Destinations, 1965 - 1995," vol. 51, 2007; Timothy J Hatton, "The Rise and Fall of Asylum: What Happened and Why?," *Source: The Economic Journal*, vol. 119, 2009; Mathias Czaika and Mogens Hobolth, "Do Restrictive Asylum and Visa Policies Increase Irregular Migration into Europe?," *European Union Politics* 17, no. 3 (2016): 345–65, https://doi.org/10.1177/1465116516633299; Tilman Brück et al., "Determinants and Dynamics of Forced Migration to Europe: Evidence from a 3-D Model of Flows and Stocks," 2018, www.iza.org.

[24] Tilman Brück et al., "Determinants and Dynamics of Forced Migration to Europe: Evidence from a 3-D Model of Flows and Stocks".

[25] Khalid Koser, "Irregular Migration, State Security and Human Security A Paper Prepared for the Policy Analysis and Research Programme of the Global Commission on International Migration and Does Not Represent the Views of the Global Commission on International Migration," 2005.

[26] Khalid Koser, "When Is Migration a Security Issue?," Brookings, 2011, https://www.brookings.edu/opinions/when-is-migration-a-security-issue/ Sergei Metelev, "Migration as a Threat to National Security," *Indian Journal of Science and Technology* 9, no. 14 (2016), https://doi.org/10.17485/ijst/2016/v9i14/91086.

escalation. Analysis is performed within the time frame 1989 - 2017. Area specification emerged directly from the problem and also helped to define scenario space. These definitions themselves determined general conceptualization of a variable for analysis - migration to the Czech Republic per year.

Data on migration are available on website of The United Nations' Refugee Agency[27]. Fig.1 presents basic extrapolation of the trend in the horizont of 5 years. This concerns the first step of TIA - establishing a trend for a particular threat identified by the country in question (Czechia):

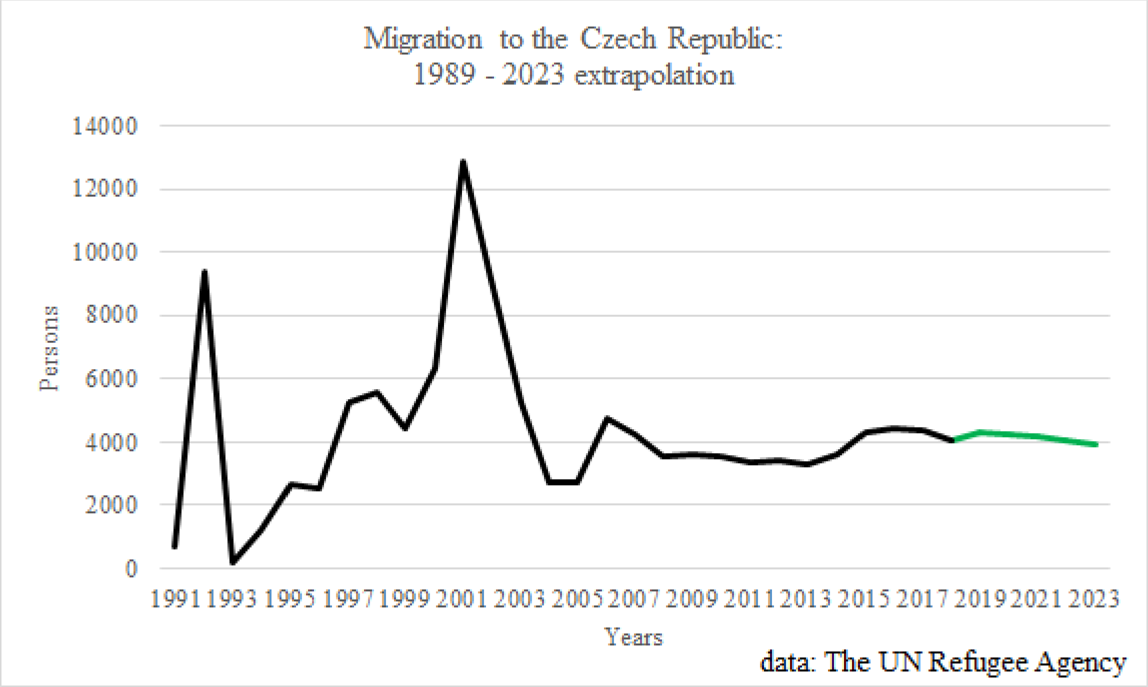


Fig. 1: Migration to the Czech Republic: 1989 - 2023 extrapolation

In classical scenario-building, at this point it is usual to engage a group of experts or confront literature in order to list a set of events which in case of occurrence would have an impact on the migration to the CR. However, keeping in mind not only general critique of possible researchers' biases and issues of validity and reliability but also one of requirements to achieve effective conflict prevention - necessity to incorporate macro environment analysis, we decided to choose a different approach in this step.

Credible capturing of the environment is challenging, it is a very tangled task which cannot be completed by neither qualitative nor quantitative methods exclusively. However if both approaches are combined, it can minimize pitfalls of an attempt to cover as much of environment complexity as possible. One of a few effective and transparent methods combining qualitative and quantitative approach is Qualitative comparative analysis. QCA is by definition qualitative a comparative methods approach. The main focus is on the systemizing of the process of comparison in order to increase the number of cases that can be actually compared. The method is still case oriented[28] but thanks to the formalized analysis by mathematical apparatus of set theory, a large number of cases can be analyzed. Therefore QCA also resembles a quantitative approach and combines the advantages of both. The main

[27] Data available on website: http://popstats.unhcr.org/en/overview.

[28] De Meur, Giséle, Benoît Rihoux, and Charles C. Ragin. "Qualitative Comparative Analysis (QCA) as an Approach," In *Configurational Comparative Methods: Qualitative Comparative Analysis (QCA) and Related Techniques*, ed. by Benoît Rihoux and Charles C. Ragin (Thousand Oaks: Sage, 2009), 1-18.

principle lies in treating the case as a combination of factors producing a specific outcome. Examined factors are the same for all cases, but factors and also outcomes may acquire different values. As every case is represented by combinations of factors, it is possible to systematically compare many complex situations. QCA comprises more techniques, often used is csQCA - QCA on crisp sets where values of factors and outcome are dichotomous[29]. The aim of the analysis is to structurally look for patterns in empirical data[30].

The method was chosen because it allows us to describe the environment of every case in detail but at the same time, the description is structured and formalized. If only experts' opinions are considered there is a change of neglecting some variables or overlooking complex relations among them. Analysis with set theory apparatus also enables testing of different combinations and evaluating their relevance.

In the case of the Czech Republic, 316 cases of escalation opportunities between 1989 - 2017 in countries of Western Europe, Postcommunist space, Middle East and North Africa were a basis for creating the QCA model. The result of the analysis is a set of causal paths leading to escalation into an armed conflict. They are combinations of economic (youth unemployment; GDP at purchasing parity power; income inequality), social and demographic (population growth; ethnic power relations), political (conflict in last 50 years in the country; conflict in neighbourhood; irredentist or secession claims; political violence and terror; repressiveness of regime; institutionalized democracy), environmental (conflict because of basic sources) and military (global militarization index) conditions. These conditions had been chosen from the larger set of possible relevant factors, the original set was composed in order to cover as broad a range of environment characteristics as possible in correspondence with literature on sources of conflict. 12 aforementioned conditions were chosen out of the set based on the results of the testing of their combinations by Boolean algebra apparatus.

Tab. 1: Conflict causal paths

No.	**Conflict causal path**
path 1	GDP_PPP*IRED_CLAIM*~TER_CLAIM*NEIGH_CONF
path 2	GDP_PPP*CONF_50*DEM_POLITY*ZAKL_ZDROJE
path 3	~GINI_DISP*EPR_ED*~NEIGH_CONF*~GMI_BICC
path 4	~GINI_DISP*CONF_50*~DEM_POLITY*ZAKL_ZDROJE
path 5	~POP_GROWTH*~EPR_ED*TER_CLAIM*PTS_S
path 6	~YUEMP*~GINI_DISP*IRED_CLAIM*~TER_CLAIM*NEIGH_CONF
path 7	~YUEMP*GINI_DISP*IRED_CLAIM*TER_CLAIM*~NEIGH_CONF
path 8	YUEMP*POP_GROWTH*~NEIGH_CONF*DEM_POLITY*~ZAKL_ZDROJE
path 9	YUEMP*IRED_CLAIM*CONF_50*NEIGH_CONF*DEM_POLITY
path 10	~GDP_PPP*EPR_ED*~TER_CLAIM*~NEIGH_CONF*~GMI_BICC
path 11	GDP_PPP*CONF_50*NEIGH_CONF*PTS_S*~GMI_BICC
path 12	GINI_DISP*IRED_CLAIM*~NEIGH_CONF*ZAKL_ZDROJE*GMI_BICC
path 13	~POP_GROWTH*IRED_CLAIM*~NEIGH_CONF*PTS_S*ZAKL_ZDROJE
path 14	~IRED_CLAIM*TER_CLAIM*NEIGH_CONF*~DEM_POLITY*ZAKL_ZDROJE
path 15	YUEMP*~GDP_PPP*GINI_DISP*POP_GROWTH*~NEIGH_CONF*GMI_BICC

[29] Berg-Schlosser, Dirk, and Giséle De Meur. “Comparative Research Design: Case and Variable Selection”. In *Configurational Comparative Methods: Qualitative Comparative Analysis (QCA) and Related Techniques*, ed. by Benoît Rihoux and Charles C. Ragin (Thousand Oaks: Sage, 2009), 19-33.

[30] Schneider, Carsten Q, and Claudius Wagemann. *Set-Theoretic Methods For The Social Sciences: A Guide To Qualitative Comparative Analysis.* (Cambridge:Cambridge University Press, 2012)

No.	Conflict causal path
path 16	YUEMP*GDP_PPP*POP_GROWTH*CONF_50*NEIGH_CONF*PTS_S
path 17	YUEMP*GDP_PPP*~TER_CLAIM*NEIGH_CONF*PTS_S*~DEM_POLITY

By discovering causal paths leading to conflict in different parts of the world (Tab. 2) many factors describing macro environment and its changes were combined into 2 types of impacting events - low intensity conflict escalation and high intensity conflict escalation. All conditions are structural, therefore their changes are not as dynamic and allow long-term analysis. On the other hand, some structural factors can be significantly changed by external impact or internal disruption. The advantage of QCA model is that such changes can be immediately incorporated and reflected in results. In this respect, the short-term aspect is also taken into consideration.

Knowing causal paths leading to the conflict escalation enables collection of more up to date data for countries of interest and checks whether any of the countries' combinations correspond with conflict causal paths. If so, it is an important early warning element because it is possible to identify potential threats in pursuance of evolution of conflict sources. It is a way to identify a potential escalation opportunity even before existing early warning systems start to detect early stages of conflict. The result of this step in analysis is not only the list of countries which may be at risk of conflict escalation but also the number of conflict causal paths which complies with the current situation in the country. The probability of escalation can be partially estimated based on simple logic, the more corresponding causal paths, the higher probability of escalation. Another part of probability estimation is focused on cases from the original set of 316 cases in model. All causal paths are empirically anchored and can be matched with particular cases in the original set and then it is possible to count the cases which correspond with the conflict causal path in the past.[31] "The strength" of the causal path can be defined by this number (Tab. 2) and the second component of probability is thus estimated.

Tab. 2: The strength of causal paths

No.	Matched cases[32]	Strength of the path
path 1	MDA2016,MDA2017	1
path 2	MLI2017	3
path 3	ISL2016,IRL2016,ISL2017,IRL2017,LUX2017	1
path 4	AFG2017,DZA2017,UKR2017	9
path 5	IRN2016,AZE2016,RUS2016,TKM2016,UZB2016, IRN2017,ARM2017,AZE2017,RUS2017,TKM2017,UZB2017	4
path 6	NOT FOUND	1
path 7	GBR2016	1
path 8	NOT FOUND	2
path 9	IRQ2016,GEO2016,IRQ2017,GEO2017	4
path 10	ISL2016,IRL2016,ISL2017,IRL2017,LUX2017	1
path 11	MLI2016,TJK2016,UZB2016,MLI2017,TJK2017, UZB2017	5

[31] The results of QCA includes for every path also calculation of the frequency of cases when conflict causal path occurred but did not lead to the escalation. If the rate exceeded 80% the causal path was not evaluated as conflict causal path.

[32] Cases codes are composed of ISO Alpha 3 countries' codes and the examined year.

No.	Matched cases[32]	Strength of the path
path 12	YEM2017	3
path 13	NOT FOUND	3
path 14	SYR2016,AFG2017,DZA2017,EGY2017,MAR2017,SSD2017,SYR2017	8
path 15	NOT FOUND	2
path 16	MLI2016,SDN2016,SSD2016,TJK2016,MLI2017, SDN2017,SSD2017,TJK2017	7
path 17	NOT FOUND	1

This approach, assessing the potential risk of conflict escalation in every country, leads to the first reduction of relevant cases which need to be reflected. It significantly decreases the number of cases which need attention and in the next step suffices to evaluate impact only for countries which were determined by previous analysis. From all countries entering the analysis, only 24 face an increased risk of conflict escalation in the examined time period (in this case 2 years). Instead of 86 cases to further evaluation, only 24 will be subjected to further analysis.[33] After the probability assessment, countries are divided into 3 groups: high probability, medium probability and low probability. The last group will be taken into consideration only if these cases have potentially significant impact on migration. The major reduction of countries staying in the "perimeter" of analysis reduces the number of scenarios needed in the final phase. It also lower expenses of early warning and conflict prevention and focus can be shifted to the operational planning and early action.

Every causal path can be matched with cases in the original set. Thanks to that, it is possible to retrospectively ascertain intensity (expressed by battle deaths) of every particular escalation and with this in mind is possible to assess potential impact of other cases of escalation via the same causal path. Many authors examined the relation between conflict intensity and the volume of migration flows and found positive correlation[34]. Conte and Migali[35] analyzed, along with many different factors, the role of the medium-level (25-1000 battle deaths) and high-level (1000+ battle deaths) conflict intensity in international migration. According to their results, high-level intensity conflicts increase the migration flow significantly more than medium-level intensity conflict. Abel et al.[36] chose a different approach, they utilized different variables for different conflict intensity but worked with only variable "Battle Deaths" and examined how relation of all independent variables to the dependent variable evolves in 2 years subperiods. Numbers differed slightly for subperiods, but in each of them the variable "Battle Deaths" had a positive influence on migration flows. The impact of the conflict on migration will be calculated for each case as the combination of the mean of coefficients presented by Abel et al.[37] and intensity of conflicts in causal path which correspond with combination of conditions in particular case. Estimated value of the

[33] MDA, MLI, ISL, AFG, IRN, GBR, TJK, IRQ, YEM, SYR, SSD, AZE, RUS, TKM, UZB, ARM, IRL, LUX, DZA, UKR, GEO, SDN, EGY, MAR.

[34] Timothy J Hatton, "The Rise and Fall of Asylum: What Happened and Why?," *Source: The Economic Journal*, vol. 119, 2009; Guy J. Abel et al., "Climate, Conflict and Forced Migration," *Global Environmental Change*, 2019, https://doi.org/10.1016/j.gloenvcha.2018.12.003; Alessandra Conte and Silvia Migali, "The Role of Conflict and Organized Violence in International Forced Migration," *Source: Demographic Research* 41: 393-424, accessed February 27, 2020, https://doi.org/10.4054/DemRes.2019.41.14.

[35] Alessandra Conte and Migali S, "The Role of Conflict and Organized Violence in International Forced Migration".

[36] Guy J. Abel et al., "Climate, Conflict and Forced Migration".

[37] *Ibidem.*

impact (the presented example uses a 3% increase) will be used to calculate the overall increase in international migration and the respective increase of migration to the Czech republic will define trend modification.

After the impact estimation for every case, particular situations for scenario-building can be chosen based on impact. Situations can be combinations of more cases, taking into account cases with high probability (even if they have low impact) but also for the cases with high impact (even if they have low probability). Estimating the other details of the impact follows - time frame of when the impact on migration becomes evident is according to aforementioned studies 1-2 years and the same is true for the highest impact - the basic surprise-free trend extrapolation can be modified. Fig. 2 presents an example of a case of South Sudan which has been attributed with a high possibility of conflict escalation and at the same time, the escalation would have considerable impact on migration flows. Modifying a trend based on the results of one country is not a complex situation for scenario-building, it merely demonstrates an increase with a single country source. The course of the trend did not change, because Fig. 2 presents a situation when South Sudan is the only country experiencing conflict escalation. If a complex situation is described (e.g. if all countries with higher probability than South Sudan or higher impact than South Sudan are included) the displayed trend would change more significantly and likely even reverse.

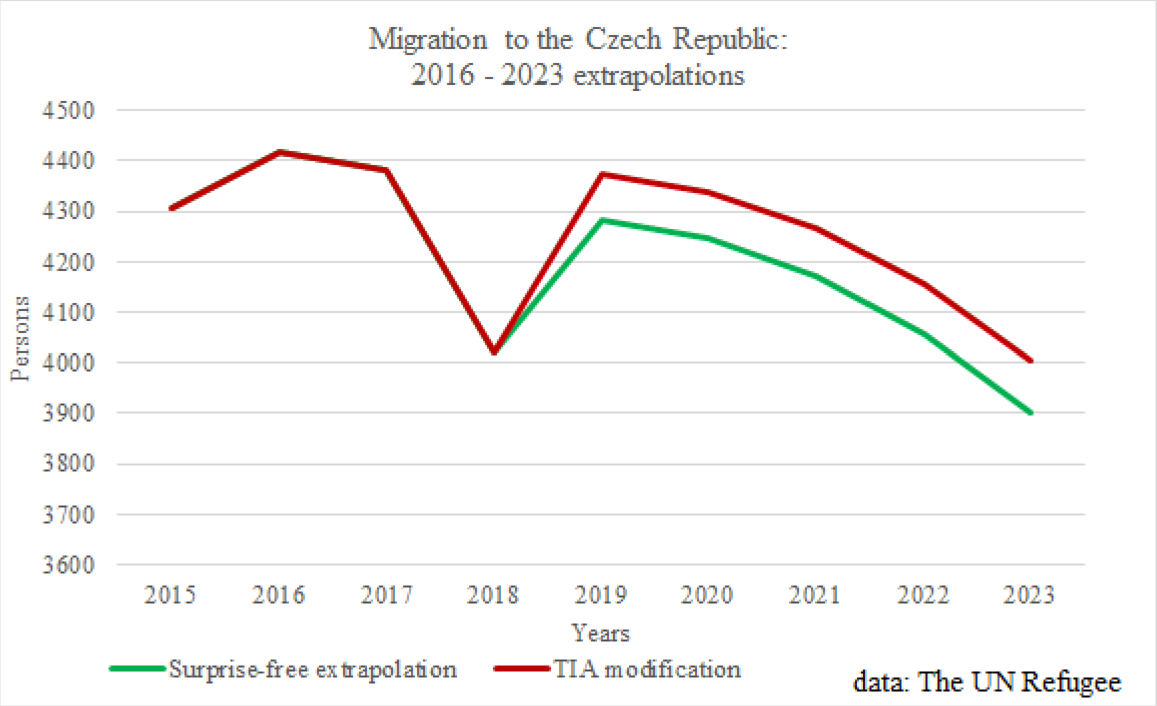


Fig. 2: Comparison of surprise-free extrapolation and Adapted-TIA trend modification

Modified trend extrapolation is the base for building a scenario. It exposes possible future dangers and leads the narrative in scenario. Using the QCA brings another advantage which is revealed in the last step. Thanks to the method's affiliation to the qualitative methods, it is case oriented and the practice of the QCA requires knowledge of every case. Familiarity with cases and their context is a very good starting position for scenario-building, it enables incorporating operational planning and setting the main course of preventive actions which are more relevant for the particular situation. Looking at the bigger picture in situations improves reactivity of the scenario and it contributes to achieving another goal of successful conflict prevention – better integration of planning and forecasting.

Conclusion

Conflict prevention needs to incorporate early warning and prediction with measures and actions addressing the identified threat to be effective. Achieving successful interconnection of both aspects is one of main goals of successful and effective conflict prevention. For smaller countries, taking into account their limited resources and the need of prioritization, scenario-building with application of Trend Impact Analysis offers a superior method. To demonstrate the relevance of the method for small states' conflict prevention and threat mitigation, an example of migration to Czechia was chosen.

Trend impact analysis in scenario-building reacts to criticism of prediction and forecasting by a systematized methodology. In order to avoid surprise-free predictions and neglecting unquantifiable variables, TIA combines quantitative and qualitative methods. However, there are still pitfalls the original TIA method does not address. It still produces a considerable amount of scenarios and by engaging experts' opinions brings back human imperfections excluded before by relying on quantitative approach in the earlier phase. To prevent these problems from decreasing effectiveness and success of conflict prevention, we decided to modify the Trend Impact Analysis technique by engaging qualitative comparative analysis into the process.

QCA has proven to be a powerful tool in decreasing the number of scenarios. The method's formalized procedure and structured results enable systematic minimization of scenarios. Unlike the current methods of minimizing the number of scenarios in TIA, which are dependent on experts' assessments, QCA-led reduction is no less based on expert knowledge than the aforementioned one but it also incorporates classical probability calculation. It has been also demonstrated how this systematic minimization reveals patterns which could have been unnoticed. The example of the Czech Republic shows that traditional focus on major conflict-prone countries like Egypt, Libya or Sudan is insufficient, and other sources of migration should be considered with assessed probabilities. Mali, Algeria or Sudan which are not primary interests of Czechia have a high probability of conflict escalation in spite of their medium impact potential. On the other hand, attention should be also paid to countries with a lower probability of conflict escalation but high possible impact such as Azerbaijan. By systematizing the procedure, we thus arrive at an impact-driven (the impact being the likelihood of armed conflict escalation) assessment surpassing the weakness of classical extrapolation techniques - the assumption that the future will be similar to the past - and better defining the source of perceived threats - in this case irregular migration.

Another articulated advantage of QCA directly addresses the main prerequisite for conflict prevention. The interoperability of predictions and planning and actions is more coherent because of QCA practice. Because of its qualitative aspect, the deep knowledge of cases is required which indirectly adds value to planning. To summarize, there are fewer scenarios which are more relevant and their impact on planning is better targeted, therefore conflict prevention has more potential to be successful.

Adapted-TIA makes the method more flexible regarding sensitivity. In every step of the analysis the researcher or examining body may control to what extent the number of scenarios will be reduced - meaning sensitivity may be adjusted by controlling thresholds of probability and thresholds of impact and setting them as low or as high as preferred. This is a highly relevant result for smaller countries which may opt for higher sensitivity in one threat area and lower sensitivity in another - yet still retaining the same methodology and procedure. On the input side, in this particular case, also the intensity of the armed conflict can be set to low, medium or high or even the combination of these intensities thus producing the desired level of sensitivity to migration.. These parameters are defined while defining the QCA model.

Incorporating Qualitative Comparative Analysis into Trend Impact Analysis based scenario-building brought significant progress in addressing issues central to conflict prevention in small countries with limited sources. The illustrated case of migration to Czechia above serves as demonstration of the transparency and systemic nature of steps in Adapted-TIA application. Engagement of QCA does not disrupt the structure of TIA technique or scenario-building, therefore suggested adaptation can be easily applied to the broad spectrum of threats. The main advantage is that the Adapted-TIA model can be further developed and trained not only to achieve better results but also to cover more topics central to conflict prevention.

BIBLIOGRAPHY

1. Abel, Guy J., Michael Brottrager, Jesus Crespo Cuaresma, and Raya Muttarak. “Climate, Conflict and Forced Migration.” *Global Environmental Change*, 2019. https://doi.org/10.1016/j.gloenvcha.2018.12.003.
2. Babbitt, Eileen F. “The Evolution of International Conflict Resolution: From Cold War to Peacebuilding.” *Negotiation Journal* 25, no. 4 (October 1, 2009): 539–49. https://doi.org/10.1111/j.1571-9979.2009.00244.x.
3. Basuchoudhary, Atin, James T. Bang, Tinni Sen, and John David. [2018]. *Predicting Hotspots: Using Machine Learning To Understand Civil Conflict*. Lanham, Maryland: Lexington Books.
4. Berg-Schlosser, Dirk, and Giséle De Meur. “Comparative Research Design: Case and Variable Selection”. In *Configurational Comparative Methods: Qualitative Comparative Analysis (QCA) and Related Techniques*, edited by Benoît Rihoux and Charles C. Ragin, 19-33. Thousand Oaks: Sage, 2009. ISBN 9781412942355
5. Bock, J. G. 2014. Firmer Footing for a Policy of Early Intervention: Conflict Early Warning and Early Response Comes of Age. *Journal of Information Technology & Politics*, 12(1), 103–111.
6. Bredel, Ralf. c2003. *Long-term conflict prevention and industrial development: the United Nations and its specialized agency, UNIDO*. Nijhoff law specials, 57. Leiden: Brill. ISBN 978-90-04-13619-9.
7. Brück, Tilman, Kai M Dunker, Neil T N Ferguson, Aline Meysonnat, and Eleonora Nillesen. “Determinants and Dynamics of Forced Migration to Europe: Evidence from a 3-D Model of Flows and Stocks,” 2018. www.iza.org.
8. Campbell, Susanna, and Patrick Meier. “Deciding to Prevent Violent Conflict: Early Warning and Decision-Making within the United Nations,” 32, 2007. https://irevolution.files.wordpress.com/2011/07/campbell-meier-isa-2007.pdf.
9. Cederman, Lars-Erik, and Nils B. Weidmann. “Predicting Armed Conflict: Time to Adjust Our Expectations?” *Science,* no. 355 (2017): 474–76. https://doi.org/10.1126/science.aal4483.
10. Conte, Alessandra, and Silvia Migali. “The Role of Conflict and Organized Violence in International Forced Migration.” *Source: Demographic Research* 41: 393–424. Accessed February 27, 2020. https://doi.org/10.4054/DemRes.2019.41.14.
11. Czaika, Mathias, and Mogens Hobolth. “Do Restrictive Asylum and Visa Policies Increase Irregular Migration into Europe?” *European Union Politics* 17, no. 3 (2016): 345–65. https://doi.org/10.1177/1465116516633299.
12. Davenport, Christina, Will Moore, and Steven Poe. “Domestic Threats and Forced Migration, 1964-1989.” *International Interactions* 29, no. 1 (2003): 27–55. https://doi.org/10.1080/03050620304597.

13. De Meur, Giséle, Benoît Rihoux, and Charles C. Ragin. "Qualitative Comparative Analysis (QCA) as an Approach". In *Configurational Comparative Methods: Qualitative Comparative Analysis (QCA) and Related Techniques*, edited by Benoît Rihoux and Charles C. Ragin, 1-18. Thousand Oaks: Sage, 2009. ISBN 9781412942355
14. Durance, Philippe, and Michel Godet. "Scenario Building: Uses and Abuses." *Technological Forecasting and Social Change,* 2010. https://doi.org/10.1016/j.techfore.2010.06.007.
15. Gross, Eva, and Ana E. Juncos. 2014. *Eu Conflict Prevention And Crisis Management: Roles, Institutions, And Policies*. London: Routledge. ISBN 9781138829893.
16. Hatton, Timothy J. "The Rise and Fall of Asylum: What Happened and Why?" *Source: The Economic Journal*. Vol. 119, 2009.
17. Hegre, H., Karlsen, J., Nygård, H. M., Strand, H., & Urdal, H. 2013. Predicting Armed Conflict, 2010–20501. *International Studies Quarterly,* 57(2), 250–270. https://doi.org/10.1111/isqu.12007
18. Herbert Wulf and Tobias Debiel. 2009. Conflict Early Warning and Response Mechanisms. A Comparative Study of the AU, ECOWAS, IGAD, ASEAN/ARF and PIF. no. Crisis States Working Papers Series No.2.
19. Huss, William R. "A Move toward Scenario Analysis." *International Journal of Forecasting*, 1988. https://doi.org/10.1016/0169-2070(88)90105-7.
20. Huss, William R., and Edward J. Honton. "Scenario Planning-What Style Should You Use?" *Long Range Planning*, 1987. https://doi.org/10.1016/0024-6301(87)90152-X.
21. Kalous, M. How (Not) to Predict the Future? Analysis of several pioneering studies in the field of Czech political and security scenario-building. *Obrana a Strategie*. 18(1):131 - 146. doi:10.3849/1802-7199.18.2018.01.131-146.
22. Koser, Khalid. "Irregular Migration, State Security and Human Security A Paper Prepared for the Policy Analysis and Research Programme of the Global Commission on International Migration and Does Not Represent the Views of the Global Commission on International Migration," 2005.
23. ———. "When Is Migration a Security Issue?" Brookings, 2011. https://www.brookings.edu/opinions/when-is-migration-a-security-issue/.
24. Metelev, Sergei. "Migration as a Threat to National Security." *Indian Journal of Science and Technology* 9, no. 14 (2016). https://doi.org/10.17485/ijst/2016/v9i14/91086.
25. Martelli, Antonio. 2014. *Models Of Scenario Building And Planning: Facing Uncertainty And Complexity*. New York: Palgrave.ISBN 978-1-137-29349-7.
26. Moore, Will H, and Stephen M Shellman. "Whither Will They Go? A Global Study of Refugees' Destinations, 1965 - 1995." Vol. 51, 2007.
27. Neukirch, Claus. "Early Warning and Early Action – Current Developments in OSCE Conflict Prevention Activities," 2013.
28. Rohwerder, B. 2015. *Conflict Early Warning and Early Response*. Governance Social Development Humanitarian Conflict Helpdesk Research Report, 13.
29. Schneider, Carsten Q, and Claudius Wagemann. 2012. Set-Theoretic Methods For The Social Sciences: A Guide To Qualitative Comparative Analysis. [1st ed.]. Strategies For Social Inquiry. Cambridge: Cambridge University Press.ISBN 9781139004244.

30. Schwenker, Burkhard, and Torsten Wulf. *Scenario-Based Strategic Planning : Developing Strategies in an Uncertain World*. Munich: Springer Gabler, 2013. ISBN 978-3-658-02874-9
31. Taleb, Nassim Nicholas. 2008. *The black swan: the impact of the highly improbable. 2nd edition.* London: Penguin. ISBN 9780141034591.
32. Wright, George, Ron Bradfield, and George Cairns. "Does the Intuitive Logics Method – and Its Recent Enhancements – Produce 'Effective' Scenarios?" *Technological Forecasting and Social Change,* 2013. https://doi.org/10.1016/j.techfore.2012.09.003.
33. Wulf, H., & Debiel, T. 2010. Systemic disconnects: Why regional organizations fail to use early warning and response mechanisms. *Global Governanc*e, 16(4), 525–547.
34. Zyck, Steven A., and Robert Muggah. "Preventive Diplomacy and Conflict Prevention: Obstacles and Opportunities." *Stability* 1, no. 1 (September 25, 2012): 68–75. https://doi.org/10.5334/sta.ac.
35. Zartman, I. William. 2015. *Preventing deadly conflict*. Malden, MA: Polity Press. ISBN 978-0745686929.

DEVELOPING PROACTIVE MINDSETS AS TOOLS FOR PREVENTING CRISES

George-Sorin MARIN
Master's student, "Crises management" programme,
Faculty of Business and Administration, University of Bucharest
marin_sorin15@yahoo.com

Abstract: *The fact that we are living in the Era of Information is undeniable. Technology seized a huge part of our daily lives, information gathering is so facile nowadays and the instant access to data makes society intellectually lazy. In brief, humans' lives got a lot easier and, at first sight, this is not a negative aspect.*
However, easy lives do not mean lack of danger. The number of current threats is potentially higher comparing to the past, potentiated by the low level of awareness and the significate degree of recklessness in society. People are getting used to reacting to threats, which makes them vulnerable to crises or to the so-called "black swans". The current reality requires us to be constantly prepared for anything that might harm us and, in this case, being reactive is simply not enough. Therefore, in the Era of Information, society must develop proactive mindsets in order to outline a new reality: the Era of Anticipation.

Keywords: *proactive; awareness; prevention; crises; risks; society.*

Introduction

”Remember, action today can prevent a crisis tomorrow”[1]. This quote belonging to the American author Steve Shallenberger captures the most important effect humans' actions can generate – the power of change. All the things we do have consequences on the world we live in, they can affect the context that surrounds us, the relations we bind and the dynamics of the everyday life. Owning such a major capability can be misleading sometimes, because the effects can have both positive and negative impacts.

The recent years were marked by major crises among the world – the conflict in Ukraine, the global refugee crisis or even the current, ongoing Coronavirus crisis are just a few examples. Whether we are talking about political instability or imbalances, social movements or violent conflicts, worldwide, in every moment there is a crisis situation going on, with a lower or a higher level of intensity. Also, the causes can vary from a natural event to human actions, but crises have a destabilizing outcome on society overall and they can lessen the national, regional or global security.

Therefore, the current security landscape's unpredictability, the unconventional character of the new challenges and threats and risks' uncontrollable diversification potentiate the probability of crises' manifestation.

The expression "the world is facing a crisis" is increasingly used in order to describe the current security environment, shaped by the challenges provoked by globalization. Nowadays, the effects of shocks taking place in a singular region or state propagate across the borders, affecting economies, citizens and countries. The growth of the global village dictates that traditionally irrelevant risks in some countries produce significant effects in other regions. The European security is facing massive threats that increase the unpredictability of the continent – armed conflicts, jihadist terrorism, cyber attacks, hybrid threats, the weakening of the disarmament efforts, energy insecurity and climate change – leading to the need of

[1] Brigham Young University-Idaho, *Proactivity*, available at https://www.byui.edu/human-resources/training-and-development/proactivity and accessed on 03.02.2020.

strengthening the available capabilities. These global threats create a "collective consciousness"[2] so complex that nobody can escape from.

In today's European society, active involvement of citizens could play a vital role in tackling social or security challenges, emanating the need to develop a more proactive civil society in Europe. Therefore, this paper aims to identify ways in which individuals can contribute to the process of crises management, influence the development of policies for this purpose and strengthen the security environment.

A theoretical and psychological framework

Barry Buzan was one of the theorists that contributed the most to the societal understanding of security. After he broadened the concept of security to assimilate political, economic, social and environmental threats[3], Buzan argued that the individual must be perceived as the main referent element for security[4]. Therefore, this correlation was the first one that connected the idea of security (in terms of national security) to the individual.

A significant part of societal constructions about how individuals behave in a crisis situation reveals that people panic in a state of helplessness, desperately needing support from the authorities. For example, in 2005, in the United States, during the Hurricane Katrina, the national authorities had to face, beside the hazard itself, a societal breakdown – individuals were portrayed as irrational and helpless[5]. Fundamentally, the thought of a crisis induces us a state of panic, a place of uncertainty and covers us with the fear of losing control.

Despite the fact that crises are sometimes inevitable, they represent a part of life and, therefore, society does not have to fear them. By preparing for crises and having a structured plan in place, humans might be able to avoid them or, at the very least, reduce their effects' intensity. However, the remark "preparing for a crisis" can be easy said but difficult to operate.

This paper focuses on a significant behavioral element that people can use in order to prevent crises or to prepare for them: proactivity. The term "proactive" was originally used in a technical sense by Paul Whiteley and Gerald Blankfort, but with a different meaning than the one we currently utilize. They characterized proactive inhibition as the "impairment or retardation of learning or of the remembering of what is learned by effects that remain active from conditions prior to the learning"[6]. Nowadays, a relevant definition for the proactive behavior refers to anticipatory, self-starting, future-focused behavior that aims to bring change in certain situations[7]. The situations previously mentioned can definitely be crisis situations and a type of proactivity can prove itself useful in managing them. A proactive behavior involves creating change, not merely anticipating it. While change can be evoked unintentionally (for a negative as well as a positive outcome), people can also engage in cognitive restructuring by psychologically reframing or reinterpreting situations[8].

[2] Durkheim, Emile, *Regulile metodei sociologice*, Cultura Națională, Bucharest, 1924, p. 32.

[3] Buzan, Barry, Waever, Ole and de Wilde, Jaap, *Security: A New Framework for Analysis*, Lynne Rienner Publishers, London, 1998, pp. 21-23.

[4] Buzann Barry et al., *Security: A New Framework for Analysis*, pp. 50-52.

[5] Tierney, Kathleen, Bevc, Christine and Kuligowski, Erica, *Metaphors Matter: Disaster myths, media frames and their consequences in Hurricane Katrina*, in Waugh, William L. (ed.), *Shelter from the Storm: Repairing the National Emergency Management System after Hurricane Katrina (Special Issue of The Annals of the American Academy of Political and Social Science Series)*, vol. 604, SAGE Publications, Philadelphia, 2006, pp. 72-74.

[6] Whiteley, Paul and Blankfort, Gerald, *The Influence of Certain Prior Conditions Upon Learning*, in *Journal of Experimental Psychology*, vol. 16, APA Publishing, 1933, pp. 843–851.

[7] Grant, Adam and Ashford, Susan, *The dynamics of proactivity at work*, in *Research Organizational Behavior*, vol. 28, Elsevier, 2008, pp. 33-34.

[8] Bateman, Thomas and Crant, Michael J., *Proactive Behavior: Meaning, Impact, Recommendations*, in *Business Horizons*, vol. 42, Issue 3, Elsevier, 1999, p. 63.

An old saying states that "the best way to manage a crisis is to prevent it; the second best way to manage it is to prepare for one"[9]. Rather than being proactive, society is usually reactive. Therefore, most of the time, the results are ineffective and inefficient responses to crisis situations. Despite the fact that major crises were experienced during history, some important lessons were not learned, both at the institutional level and the societal one.

Times have changed and living in the current reality implies living in an era on insecurity, an era of uncertainty, nurtured by unexpected disasters, catastrophes and crises. According to Maslow's hierarchy of needs, at the base of the "pyramid" are situated the physiological and the safety human needs[10]. Physiological needs, considered universal human needs, refer to the internal motivation and they consist in food, water, warmth and rest. Once a person's physiological needs are relatively satisfied, their safety needs dominate behavior. Our safety needs appear in the early childhood, since children have a need for safe, predictable environments and they naturally react with fear or anxiety when these are not met. Maslow pointed out that safety needs of the adults living in developed nations are more apparent in emergency situations such as wars and disasters[11]. Briefly, the safety and security needs include health, employment, property, family and social stability.

Therefore, humans will naturally tend to satisfy these two categories of needs, leading to the hypothesis in which, correctly conducted, the human brain can assess and manage the potential weaknesses, vulnerabilities and issues, at least at an individual level. A small impulse coming either from an external actor or from the individual himself can model the human nature's reporting to risks and threats, especially in the context of what is known as the "risk society".

The survival of the risk society: preventive thinking and acting

Risk society refers to a sociological theory developed by Ulrich Beck, invoking "a systematic way of dealing with hazards and insecurities induced and introduced by modernization itself"[12]. Beck divides modernity into sub-periods: first modernity (containing early modernity – from 1500's to about 1800 – and high modernity – 1800 to 1960 –) and second modernity (since 1960 to present), which he describes as a risk society[13]. The main idea of Beck's theory is that new risks require society to reconfigure itself in order to deal with them.

While a proactive approach focuses on mitigating problems before they appear, a reactive approach is based on responding to events after they have happened. Therefore, the biggest difference between these approaches is the perspective humans provide in assessing risks, threats, actions or events. The proactive thinking approach encourages taking responsibility for one's life or for society, meaning that proactive people think before they act. They recognize they cannot control everything that happens to them, but they can control what they do about it.

When addressing the United Nations General Assembly in 1999, Secretary General Kofi Annan cautioned that "building a culture of prevention is not easy. While the costs of prevention have to be paid in the present, its benefits lie in a distant future. Moreover, the

[9] Frandsen, Finn and Johansen, Winni, *Organizational Crisis Communication*, SAGE Publications, Croydon, 2017, p. 70.

[10] Maslow, Abraham, *A theory of human motivation*, in *Psychological Review*, vol. 50, Issue 4, APA Publishing, 1943, pp. 370-377.

[11] Silton, Nava, Flannelly, Laura, Flannelly, Kevin and Galek, Kathleen, *Toward a Theory of Holistic Needs and the Brain*, in *Holistic nursing practice*, vol. 25, Lippincott, Williams & Wilkins Publishing, 2011, pp. 258-259.

[12] Beck, Ulrich, *Risk Society: Towards a New Modernity*, SAGE Publications, London, 1992, pp. 21-22.

[13] Beck, Ulrich and Lau, Christoph, *Second modernity as a research agenda: theoretical and empirical explorations in the 'meta-change' of modern society*, in *British Journal of Sociology*, vol. 56, no. 4, 2005, pp. 525-557.

benefits are not tangible; that are the disasters that did not happen"[14]. Thereby, decision makers face a politicians' dilemma about funding pre-disaster risk awareness and risk reduction measures.

On the other side, individuals might think that it is not their duty to protect themselves against high-risk national security threats such as terrorist attacks. The popular perception is that this is exclusively the national authorities' job or it is the intelligence services' desideratum to prevent and counter the terrorist phenomenon, due to their resources and powers.

Preponderantly, this affirmation is a true fact, but citizens can significantly help to reduce the threat generated by terrorism or extremism. No intelligence service or law enforcement agency can effectively protect the national security without the support and cooperation of the citizens they serve. Therefore, existing and orienting oneself in this world increasingly involves an understanding of the confrontation with catastrophic risks[15].

Most people do not dare to pick up their ideas for a better and safer society and put them in practice, due to the lack of confidence or the indecisiveness to choose the right momentum to get started. That is why state institutions may resort to a number of techniques to increase social involvement in risk assessment and crisis management, from the ordinary but very important process of information exchange to the creation of citizen advisory committees and citizen cadre opportunities.

Prevention consists in early interventions before any illegal activity takes place. Reporting suspicious activities can help in the process of disrupting the terrorist activities and planning cycles. The societal support on this particular issue is much more relevant considering the fact that most terrorist acts are well organized and well planned. Being proactive is the only choice society can resort to – although it is the intent of the terrorist to instill fear in you, it is your vigilance that the terrorist fears the most[16]. "If You See Something, Say Something" is the motto of a Homeland Security's awareness campaign launched in July 2010. The campaign aimed to be a simple and effective program with the purpose to raise public awareness of indicators of terrorism/terrorism-related crime and to emphasize the importance of reporting suspicious activity to the proper state and local law enforcement authorities[17].

Furthermore, the campaign encourages citizens to report suspicious activities to local law enforcement or persons of authority using the 5W's: *who?* (did you see), *what?* (did you see), *when?* (you saw it), *where?* (it occurred) and *why?* (it's suspicious). Having the 5W's always in mind is one of the first steps to becoming proactive, regardless of the circumstances. A society whose collective mindset is reported to the 5W's is rather a proactive one and it is more likely to prevent a massive shock or to be prepared for it in case it occurs.

Enabling thinking about problems and dangers more frequently and in a more profound way and considering that many risk factors may not be intuitively apparent will provide us with a better awareness of our environment. Since we live in a knowledge based society, in an Era of Information, the more critical we think the more superior our knowledge will be.

[14] UN Office for Disaster Risk Reduction, *International Strategy for Disaster Reduction: Newsletter for Latin America and the Caribbean*, Issue 15, 1999, available at https://www.eird.org/eng/revista/No15_99/pagina1.htm and accessed on 12.02.2020.

[15] Beck, Ulrich, *Critical Theory of World Risk Society: A Cosmopolitan Vision*, Blackwell Publishing, Oxford, 2009, p. 6.

[16] The Irvington Police Department, *Safeguard New York*, n. d., available at http://www.irvingtonpolice.com/files/Safeguard_Mass_Transit_1_.pdf and accessed on 14.02.2020.

[17] The Department of Homeland Security, *If You See Something, Say Something Campaign Overview*, 2015, available at https://www.dhs.gov/publication/if-you-see-something-say-something™-campaign-overview and accessed on 14.02.2020.

A European institutional approach

One of the main objectives set at a European institutional level is raising the proactive citizen involvement in the functioning of the supranational organization, including their contribution to the risk management process.

Since chemical, biological, radiological and nuclear risks represent a major concern for the European Union, one way to reinforce the role of professionals is by preparation and civil society engagement. In 2012, the Community Research and Development Information Service (CORDIS) launched the EU-funded PROACTIVE project, aiming to enhance preparedness against chemical, biological, radiological and nuclear security risks and the overall Security Union approach to fight crime and terrorism by increasing practitioner effectiveness in managing large, diverse groups of people[18].

The project provides human-centred recommendations for EU standards concerning the integration of chemical, biological, radiological and nuclear technologies and innovations that are better adapted to the needs of all citizens.

In the recent years, various policy documents of the Organization for Security and Co-operation in Europe (OSCE) have firmly encouraged participating states to proactively engage civil society and other community actors into the organization's efforts to prevent and counter violent extremism and radicalization that lead to terrorism.

In 2018, OSCE the published a guidebook for South-Eastern Europe, entitled "The Role of Civil Society in Preventing and Countering Violent Extremism and Radicalization that Lead to Terrorism". The document defines civil society as "a diverse body of civil actors, communities and formal or informal associations with a wide range of roles, who engage in public life seeking to advance shared values and objectives"[19].

Besides the European Union and OSCE, nongovernmental organizations also have a huge impact on the societies' risk assessment processes. One tangible example is the Society for Risk Analysis – Europe (SRA-E), that aims to bring together individuals and organizations interested in risk analysis/management/assessment/governance/communication in Europe. The interdisciplinary society encourages all the citizens interested in studying risks to communicate, cooperate and develop new methodologies for risk management[20], emphasizing with the European dimension in the promotion of interdisciplinary research and education.

Developing proactive communication with citizens

Social media data is viewed as an essential resource for emergency response operations. Over the last years, the use of social media has gained the attention of professionals operating in crises response organizations and institutions. In the crisis management literature, it has been recognized for decades that citizens are self-reliant when there is social disruption and in crisis situations, whether those are incidents, emergencies or large-scale disasters[21]. Therefore, social media platforms provide a significant opportunity for people to keep each other informed and for governments to dispose additional resources in crisis response situations.

[18] CORDIS, *PRedictive reasOning and multi-source fusion empowering AntiCipation of attacks and Terrorist actions In Urban EnVironmEnts*, 2015, available at https://cordis.europa.eu/project/id/285320 and accessed on 18.02.2020.

[19] OSCE, *The Role of Civil Society in Preventing and Countering Violent Extremism and Radicalization that Lead to Terrorism*, 2018, available at https://www.osce.org/secretariat/400241?download=true and accessed on 20.02.2020.

[20] Society for Risk Analysis, *Who we are*, available at http://www.sraeurope.eu/who-we-are and accessed on 21.02.2020.

[21] Boersma, Kees, Ferguson, Julie, Diks, Dominique and Wolbers, Jeroen, *From Reactive to Proactive Use of Social Media in Emergency Response: A Critical Discussion of the Twitcident Project*, in Gilbert, Silvius (ed.), *Strategic Integration of Social Media into Project Management Practice*, IGI Global, Hershey, 2016, pp. 236-237.

While one of the biggest issues governments face is to maintain clear and direct communication with their citizens, the technologization and the rise of the digital age can outline the optimal solution to this issue. The tools that can be used to address this problem and employ a better and proactive communication consist of different digital and online solutions that the majority of the citizens can access.

For example, Community Engagement Solutions (CES) can establish collaboration between local/national institutions, higher education organizations and large communities. CES encourage ongoing discussions, are inclusive and allow the connections between governments and citizens on important issues, as they take part in public consultations.

On that note, Citizen Request Systems provide citizens with a facile way to report issues and a streamlined channel for government staff to provide updates[22]. The solution improves a two-way communication between citizens and government, allowing residents to send reports and information to the correct government entity through digital means and also to track these reports, so they can follow them all the way through to completion.

Some relevant e-government tools also include polls and surveys, essentials for getting feedback and for giving the residents an opportunity to share their views on different matters and issues.

Social media – its success is that it makes connecting so simple. Generally, we experience crises through the media and the Internet. This aspect can be used the other way around, as a key to proactive communication for governments to focus on building a well-rounded solution for managing potential crises. Social media is, at the moment, the key to good governance, since it helps the governments agencies to make a real and consolidated relationship with their citizens. When governments try to build a social media presence this is called a proactive social community management. Thus, social media can play an essential role in political mobilization and it unquestionably has a transformative effect on the organization of collective action.

However, this this digital era, both proactive and reactive social strategies are important and they should work together, because neither one will accomplish strategic risk management goals by itself. The use of social media can enable the sharing of social security information in an efficient and effective manner, responding to citizens' questions quickly and building trust within communities and governments.

An integrated approach requires analyzing the relationship between technology, people and cities/regions from a perspective centered on citizenship, similar to the philosophy of the Smart City, whose development has been possible from the point of view of technology and Big Data. Decision making acquired new participation and accountability systems that imply the empowering of the citizens. The concept supports the citizens that desire to actively participate in the decisions that affects them, including those regarding the risks and threats that can negatively influence their existence.

Conclusions

We live in a world out of control. Many risks that we confront at the moment are global by their nature. The Era of Information is defined by a multitude of dangers and threats and we have to adapt to it, to predict its changes and positively influence its process.

The polarization of risks expands the need of proactiveness within societies and a more acute awareness. There are factors that we, as single individuals, generally cannot control, such as climate change, population growth, the global economy or the technological

[22] Civic Live, *Four Tools to Make Proactive Communication with Citizens Easy*, n. d., available at https://www.civiclive.com/resources/Four-Tools-To-Make-Proactive-Communication-Easy and accessed on 25.02.2020.

disruption. Therefore, we are vulnerable to the risks associated with the future evolutions of these factors.

However, we are able to control some elements and shape their evolutions to a greater or lesser degree. Our current actions can have impact on structural measures or on community education, for example, and we, as individuals, can support decision-making one way or another.

The risks of modern society are surrounding us and we must learn to live with them and to try to reduce their probabilities and impacts to a minimum level and actively use the tools of crisis and risk management. Risk and crisis management require an integral approach (from state, corporate and citizens perspectives) due to the high environmental, human, legal and financial implications it contains. Citizen involvement in this whole process has a fundamental role, circumscribed to the phrase "we are the people – we are the government".

Combining the government and individuals' duties in the process of preventing risks is the key to effectively chart the coordinates of a safer reality – the Era of Anticipation – in accordance with Theodore Roosevelt's motto: "the best thing we can do is the right thing, the next best thing is the wrong thing, and the worst thing we can do is nothing"[23].

BIBLIOGRAPHY

1. Bateman, Thomas and Crant, Michael J., *Proactive Behavior: Meaning, Impact, Recommendations*, in *Business Horizons*, vol. 42, Issue 3, Elsevier, 1999.
2. Beck, Ulrich and Lau, Christoph, *Second modernity as a research agenda: theoretical and empirical explorations in the 'meta-change' of modern society*, in *British Journal of Sociology*, vol. 56, no. 4, 2005.
3. Beck, Ulrich, *Critical Theory of World Risk Society: A Cosmopolitan Vision*, Blackwell Publishing, Oxford, 2009.
4. Beck, Ulrich, *Risk Society: Towards a New Modernity*, SAGE Publications, London, 1992.
5. Boersma, Kees, Ferguson, Julie, Diks, Dominique and Wolbers, Jeroen, *From Reactive to Proactive Use of Social Media in Emergency Response: A Critical Discussion of the Twitcident Project*, in Gilbert, Silvius (ed.), *Strategic Integration of Social Media into Project Management Practice*, IGI Global, Hershey, 2016.
6. Buzan, Barry, Waever, Ole and de Wilde, Jaap, *Security: A New Framework for Analysis*, Lynne Rienner Publishers, London, 1998.
7. Durkheim, Emile, *Regulile metodei sociologice*, Cultura Națională, Bucharest, 1924.
8. Frandsen, Finn and Johansen, Winni, *Organizational Crisis Communication*, SAGE Publications, Croydon, 2017.
9. Grant, Adam and Ashford, Susan, *The dynamics of proactivity at work*, in *Research in Organizational Behavior*, vol. 28, Elsevier, 2008.
10. Griggs, Francis, *Citizenship, Character, and Leadership: Guidance from the Words of Theodore Roosevelt*, in *Leadership and Management in Engineering*, 2013.
11. Maslow, Abraham, *A theory of human motivation*, in *Psychological Review*, vol. 50, Issue 4, APA Publishing, 1943.

[23] Francis Griggs, *Citizenship, Character, and Leadership: Guidance from the Words of Theodore Roosevelt*, in *Leadership and Management in Engineering*, 2013, p. 247, available at https://ascelibrary.org/doi/pdf/10.1061/%28ASCE%29LM.1943-5630.0000237 and accessed on 26.02.2020.

12. Silton, Nava, Flannelly, Laura, Flannelly, Kevin and Galek, Kathleen, *Toward a Theory of Holistic Needs and the Brain*, in *Holistic nursing practice*, vol. 25, Lippincott, Williams & Wilkins Publishing, 2011.
13. Tierney, Kathleen, Bevc, Christine and Kuligowski, Erica, *Metaphors Matter: Disaster myths, media frames and their consequences in Hurricane Katrina*, in Waugh, William L. (ed.), *Shelter from the Storm: Repairing the National Emergency Management System after Hurricane Katrina (Special Issue of The Annals of the American Academy of Political and Social Science Series)*, vol. 604, SAGE Publications, Philadelphia, 2006.
14. Whiteley, Paul and Blankfort, Gerald, *The Influence of Certain Prior Conditions Upon Learning*, in *Journal of Experimental Psychology*, vol. 16, APA Publishing, 1933.
15. Website of Brigham Young University-Idaho, URL: https://www.byui.edu/human-resources/training-and-development/proactivity.
16. Website of Civic Live, URL: https://www.civiclive.com/resources/Four-Tools-To-Make-Proactive-Communication-Easy.
17. Website of OSCE, URL: https://www.osce.org/secretariat/400241?download=true.
18. Website of the Department of Homeland Security, URL: https://www.dhs.gov/publication/if-you-see-something-say-something™-campaign-overview.
19. Website of the European Union, URL: https://cordis.europa.eu/project/id/285320.
20. Website of the Irvington Police Department, URL: http://www.irvingtonpolice.com/ files/Safeguard_Mass_Transit_1_.pdf.
21. Website of the Society for Risk Analysis, URL: http://www.sraeurope.eu/who-we-are.
22. Website of the UN Office for Disaster Risk Reduction, URL: https://www.eird.org/eng/revista/No15_99/pagina1.htm.

THE CRISIS MANAGEMENT CONTINUUM: UNDERSTANDING THE IMPORTANCE OF CONFLICT PREVENTION MECHANISMS DURING PEACE TIME

Lisa-Maria ACHIMESCU
Ph.D., National Defence University "Carol I"
lisa.achimescu@gmail.com

Teodor FRUNZETI
General (ret.) professor habil., Ph.D.,
"Titu Maiorescu" University
Academy of Romanian Scientists
tfrunzeti@gmail.com

Abstract: *Crisis management must be understood as a continuum: it does not begin with conflict, nor does it end with peace. Within our scientific enquiry we aim to highlight the importance of conflict prevention mechanisms during peace-time, with special emphasis on legal and political instruments within international organizations, such as the UN, the EU. By understanding how complex normative bodies or high level political commitment contributes to the fundamental pillars of international security and stability we can strengthen crisis management mechanisms and processes. Furthermore, it is specifically relevant that we understand how crisis management, as a process, is made subject to internationalization within a fragmented legal order, making the challenges in achieving security goals all the more complex and multilayered.*

Keywords*: crisis-management, peace time, internationalization, fragmentation, continuum.*

Introduction

In the opening of the 2017 introduction to crisis management course held at the "Carol I" National Defence University, Professor Daniel Ghiba stated that *to start applying the philosophy of crisis management only when the conflict has escalated is a failure in itself.* Crisis management is usually referenced in direct relation to conflict prevention, and it is in this conceptual framework that its' true substance is revealed. In truth, crisis management is a continuum, because crisis is a constant. Whether latent, potential, even hypothetical, the funeral light of crisis beams through the cracks of bad instructional choices, insufficient investment in the promotion of human rights and welfare of people or the heavy burden of historical wrongs impossible to forget and which seem irreconcilable at an initial glance.

It is in this arid environment that the fertile idea of approaching international relations, the very maintenance international peace and security, as stated in the preamble of the normative corollary of the modern world, The Charter of the United Nations, becomes not a singular act, but a continuous effort to preserve the peace, to promote the ideas of equality and to create an environment that thrives on cooperation rather than confrontations.

Embedding our thought patterns with the notion that all actions are directed at maintaining the peace continuum *in equilibrium* creates the elasticity of international relations and brings international institutions to the forefront of the peace process.

Faced with the complexity of the current international crises, it seems necessary to create a comprehensive theoretical basis making it possible to favor strategies bringing together all the diplomatic, financial, civil, cultural and military instruments, as well in the phases of appropriate prevention and management of crises, but also the sequences of stabilization and reconstruction after a conflict.

The core purpose of the *International Crisis Management* theory is to deepen specific and specialized subjects in crisis management today[1], to acquire up-to-date and precise information, on issues of immediate concern and to put in direct contact the actors concerned.

In everyday language, a crisis constitutes a sudden change, often decisive, favorable or unfavorable, a brief, sudden or a violent attack, a decisive or perilous period of existence, a shortage or insufficiency of important or vital raw materials, food, strategic resources etc. Politically and internationally, it represents a disruption of balance, an intermediate period, characterized by a brief, sudden and violent outburst. To understand a crisis, it os therefore necessary to grasp all its dimensions and understand the disruptive and triggering factors which can lead to appeasement, stagnation or open conflict. It is also necessary to understand its actors, their motivations, their instrumentalization by other actors, and the media coverage of the phenomenon, which although external to the crisis has the potential of ultimately obscuring the origins of the crisis. Finally, to understand a crisis is also necessary to analyze the impact of external actors, whether recognized or not by the international society.

Today's international society is marred by a plethora of crises: planetary crises (*e.g* energy crises, health crises, economic crises), international political crises (*e.g* Iraq), regional political crises (*e.g* Sudan, West Africa) and local political crises (*e.g* Haiti). All these crises can remain in a latent state or can turn into often very deadly conflicts, often fought with rudimentary means. It is a question of precisely understanding its origins and reality. State-actors and the various international institutions cannot do without the development of crisis management theory which conditions the intervention procedures, the specific instruments at their disposal, the working methods, the financial means and the type of political, economic and social transition to be put in place. The management of crises conditions and resolution is crucial as long as their trajectories are never linear. Moreover, the complexity of a crisis has generated a complexity of its management, of the international systems necessary to control it, which sometimes are inadequately equipped and poorly coordinated.

The main problem consists in the fact that some of the international institutions responsible for crisis management are still unsuitably equipped to analyze, alert and adapt to crisis. Reflections on the crisis phenomenon also represents a reflection on the strategy to end the crisis, both at the level of local actors and of committed international actors. The crisis management strategy no longer means the withdrawal of a state-actor or an organization after intervention, but the establishment of a peacebuilding strategy that can lead to a gradual reduction in the presence of the international community. The crisis exit strategy is an intrinsic part of a *continuum* in managing a crisis or conflict. Today it is no longer a question of interposing between parties to a conflict, of maintaining peace in a static manner, but of developing programs which rebuild a society in crisis or a failed state, building the unfortunately ever brittle peace process. Crisis exit strategies are therefore long-term strategies, meaning long-term engagement strategies, which must allow the coordination of the international community efforts as crisis management constitutes one of its main challenges.

We used to summarize the articulation periods of a crisis under the troika *Emergency-Rehabilitation-Development*. As of late, we have started to finally add the word *prevention*. To address this articulation of different periods of a crisis, we will mention the following four main issues: the typology of crises, the *fast- and slow-burning crises*[2], the distinction between

[1] Coman, R*., "Why and how do think tanks expand their networks in times of crisis? The case of Bruegel and the Centre for European Policy Studies",* Journal of European Public Policy, Taylor & Francis Online Review, 2018.

[2] A proposed framework in order to better understand crises distinguish between how they are comprehended as "fast-burning" and "slow-burning" phenomena. Those who view crises as fast-burning typically rally material and ideational resources to address issues with high political intensity. When a crisis is perceived as slow-

continuum and *contiguum*[3], and, finally, prevention as a link between emergency and development.

Presenting the articulation between the periods of the crisis first requires reiterating that there is no such a thing as a "standard crisis". An initial typology makes it possible to distinguish five types, even if the classification exercise is always perilous: consular crises, crises linked to armed conflicts, natural disasters, health crises including food crises as well as epidemics of viral or bacteriological origin and technological disasters.

Consular crises are clearly separate because they concern the repatriation of foreign nationals staying in a country affected by one of the other four crises. They are a one-off action benefiting from strong attention from the public authorities of the sate of origin and requiring few intervening actors. Beyond the fact that a state must provide protection measure for its own citizens, we must remain attentive to the fate of nationals of developing and poor countries, stranded in an affected state, and without immediate solution. It is the mandate of the International Organization for Migration (IOM)[4], to deal with such situations and other state-actors have often been willing to have shared their capabilities with other less organized third countries.

For the other four types of crisis, we generally speak of a *continuum* because it is recognized that a single emergency response is not nearly enough. They must be dealt with over a prolonged period of time and the *per se* management of the crisis is followed by a series of activities; we are especially referring to a lasting humanitarian action that goes far beyond media coverage and public relations management.

Humanitarian action in crisis management must be sustainable as this is exactly the case in which we are talking about a *continuum*. In reality, if we wanted to be more precise and not enclose humanitarian crisis management in a bubble, we should rather speak of *contiguum* for at least three reasons.

A first reason is the increasingly frequent juxtaposition of successive crises. This may cause us to simultaneously manage an ongoing, heightened crisis when already engaged in the resettlement phase for the previous one, sometimes affecting the same victims from the same region.

The second reason constitutes the link between the time management of the crisis and its period of development. The crisis management cycle represents a fracture in the development curve. The period of development can be suddenly torn apart by the emergence of the crisis and can be slowed down by the *humanitarian intervention*. The development curve is influenced by the intensity of the crisis determining the humanitarian response by compiling the efforts of victims and of those who help them.

The third reason why we should think more of a *contiguum* than a *continuum* is the role of prevention. Risk prevention of conflicts or disasters is essential for both the development and emergency stages of a crisis. Armed conflicts are a reminder of the need for the *law of war*. Before conflicts arise, state-actors must respect their commitments to apply international humanitarian law (IHL)[5] based on the Geneva Conventions. The first basic principle of IHL consists in the distinction between civilian and military objectives. But in nowadays' reality, civilians are those who bear the brunt of war and armed tension. Thus, if

burning, the key concern is with how the issue is framed and how social expectations are changing. Thinking of fast- and slow-burning crises permits analytical distinctions in how authorities and social actors view crises and how they consider actual conditions and future narratives. The framework assists in specifying how authorities and expert and civil society groups develop policy programmes and frames, as well as changes to European societies' experiences and expectations; *see* Leonard Seadbrook, Eleni Tsingou, *"Europe's fast- and slow-burning crises",* Journal of European Public policy, vol. 26, Issue no. 3, 2019.

[3] Latin for bordering on, neighboring, contiguous.

[4] International Organization for Migration herein after "IOM".

[5] International Humanitarian Law hereinafter "IHL".

the International Committee of the Red Cross (ICRC)[6] is vigilant in helping state-actors in training their armed forces, police etc. the respective provisions of IHL, we note a real vacuum in bringing awareness of IHL norms to failed sates or third-world countries. This vacuum calls for a measurable response dedicated to crisis management in terms of prevention; indeed, the widest possible dissemination of IHL represent an essential part not only of the prevention of conflicts, but also of war crimes. Once the conflict is over, during the crisis' decline or reduction, the principle of prevention is found again through disarmament programs and the reintegration of combatants.

The United Nations

Since the dawn of human history, power has always been associated with military force. Ultimately, the ability to impose a specific behavior on the others, as well as the ability of the other to resist that will, depended on the ratio of military forces. If the development of the East-West system marks the end of the idea of global confrontation as a model of conflict since the end of the Second World War, we can ponder about the changes that have occurred since the end of the 1980s concerning the status of the conflict itself and the role of military power in international relations.

Some doctrinarians may have believed that the global society was in the process of progressive unification around common values (*e.g* free trade, democracy) and that this political and economic unification would naturally be extended in the form of common rules for managing international conflicts. The last years of the 1980s and the first of the following decade were thus those of the so-called "spring of the UN", characterized by an exceptionally consensual atmosphere that prevailed within the Security Council and, for the first time since the signing of the United Nations Charter, the maintenance of peace and international security by the mechanisms of collective security seemed to be at hand. An unexpected consequence was the fact that these years were also marked by the return of the military to the fore. With the inhibition of nuclear deterrence lifted, new windows of opportunity open up for the armed forces, especially for the middle powers, severely restrained since the Suez crisis[7].

Another consequence of these developments is that the use of military force, which constitutes one of the most important attributes of sovereignty, must increasingly be decided and implemented in a multinational framework. There are two reasons for this change. The first is of a pure technical nature: apart from the United States, no state alone has sufficient means to project a significant force, for a long period, far from its national territory. The second reason is political: state-actors are increasingly reluctant to take action that would not be legitimized by a UN mandate. Most of the time, the search for legitimacy involves the constitution of multinational coalitions.

The UN legal framework is defined by Article 53(1) of Chapter VIII of the United Nations Charter[8] which stipulates that the Security Council may use, when it deems it appropriate, such regional organizations or agencies for coercive actions carried out under its authority. From the outset, in the logic of collective security which animated them, the

[6] The International Committee of the Red Cross hereinafter "ICRC".

[7] The Suez Crisis, or the Second Arab–Israeli war, also called the tripartite aggression in the Arab world and Sinai War in Israel, was an invasion of Egypt in late 1956 by Israel, followed by the United Kingdom and France.

[8] UN Charter, Article 53(1): "The Security Council shall, where appropriate, utilize such regional arrangements or agencies for enforcement action under its authority. But no enforcement action shall be taken under regional arrangements or by regional agencies without the authorization of the Security Council, with the exception of measures against any enemy state, as defined in paragraph 2 of this Article, provided for pursuant to Article 107 or in regional arrangements directed against renewal of aggressive policy on the part of any such state, until such time as the Organization may, on request of the Governments concerned, be charged with the responsibility for preventing further aggression by such a state."

drafters of the Charter had therefore imagined that the United Nations could "subcontract" the use of force by means of regional organizations. The international milieu would soon offer multiple opportunities to apply this provision.

2015 was the year of three major reviews conducted simultaneously on peace and security in the UN system. The institutions and mechanisms put in place to achieve and consolidate peace operate according to a multilateral logic of a bygone era, while depending too much on the mitigation of crises once they arise rather than approaches to peace and security that are long-term and sustainable. The *Independent high level group* responsible for studying the peace operations concluded that the efforts of prevention "remain unsatisfactory compared to better-resourced peace operations that are deployed during and after an armed conflict"[9]. A militarized vision of conflict prevention underestimates the transformative vision of a more egalitarian world, fairer and more peaceful which is that of Resolution 1325[10], and neglects a proven and available tool for accomplish this goal. Resolution 1325 of the Security council reaffirms the important role that women play in the conflict prevention and resolution and in peacebuilding and stresses the importance of their participation on an equal footing in all efforts to maintain and promote peace and security and that they are fully associated with it, and that they should be more involved in decisions taken for the prevention and settlement of disputes.[11]

The use of armed conflict, whatever underlying causes, has a disastrous impact on the sate-actors it affects. The economic costs, the long-term implications for public institutions and the normalization of violence accompanied by its related effects represent only a few repercussions of the conflict. Fragile and failed states affected by conflicts ranked among the poorest in terms of achieving the Millennium Development Goals.[12] As noted in the report of the Expert Advisory Panel for the 2015 Peacebuilding Review by Felicity Ruby, Secretary-General of the International League of Women for Peace and Freedom at the time of the adoption of the resolution 1325: "The adoption of resolution 1325 by the Security Council marked a turning point that we can rightly welcome, but we must also use it to challenge the foundations of commercialization and militarization of international peace and security"[13].

The Secretary General's Good Offices represent a significant tool for resolving conflicts through of preventive diplomacy. This tool has been increasingly used and its expanded use during the last twenty years, and successive Secretaries General, their envoys and senior officials of the Secretariat have attempted to mediate in virtually every major armed conflict on the UN program.[14] As noted in Chapter 10: "Interveners and key stakeholders in this report, the United Nations must do more to ensure that women hold positions of responsibility and management, especially with regard to the Good offices of Secretary General where today only four women sit on a staff of 18 members".[15]

Local women's and civil society organizations are developing comprehensive peacebuilding strategies and promoting essential conflict prevention methods at local level. These efforts have also been recognized by the Security Council in its resolutions and in

[9] *Uniting Our Strengths for Peace - Politics, Partnership and People*, UN Document A / 70/95 – S / 2015/446 (Independent high-level group to review United Nations peace operations, 16 June 2015), para. 62.

[10] UN Security Council, Security Council resolution 1325 (2000) [on women and peace and security], 31 October 2000 S/RES/1325, 2000.

[11] *See* Resolution 1325 of the UN Security Council.

[12] "Fragile and Conflict-Affected States: Signs of Progress to the Millennium Development Goals", The World Bank, May 2, 2013, http://www.worldbank.org/en/news/press-release/2013/05/02/fragile-and-conflictaffected-states-signs-of-progress-to-the-millenniumdevelopment-goals.

[13] Felicity Ruby, "Security Council Resolution 1325: A Tool for Conflict Prevention?", *in* Rethinking Peacekeeping, Gender Equality and Collective Security, 2014, p. 182.

[14] "Report of the High-Level Independent Panel on United Nations Peace Operations", 2015, para. 67.

[15] *Ibidem.*

particular resolution 2171 (2014)[16], as well as in the review of the United Nations peacebuilding system[17]. In Liberia, Palava[18] or "peace huts" have been established as safe spaces where women can come together to mediate and resolve community disputes, including in the event of incidents of gender-based violence.[19]

In late 2013, the Secretary-General launched the initiative "Human rights first", with the aim of ensuring that the UN system takes effective and swift action, as required by the Charter and UN resolutions, to prevent or respond to large-scale violations of human rights or international humanitarian law. As the United Nations works to implement this initiative, including through its high-level advisory group, it must also ensure that gender analysis is integrated into all areas of action and that the recommendations pay particular attention to promoting and protecting the human rights of women. It is also important to understand the gender dimension of the human rights violations that are being monitored in order to trigger a system intervention.[20]

The International Court of Justice

The International Court of Justice (ICJ)[21] could not remain indifferent to the successive crises which shook the Balkans. Applications were made in 1993 by Bosnia and Herzegovina then six years later by Croatia, April 29, 1999, against the Federal Republic of Yugoslavia. Yugoslavia lodged a complaint against ten member countries of the North Atlantic Treaty Organization (NATO)[22], which, following the failure of the *Rambouillet Agreement*[23], decreed the initiation of air strikes on Yugoslav territory.

These proceedings have in common the fact that all three alleged violations of the The Convention on the Prevention and Punishment of the Crime of Genocide of December 9, 1948[24], positioning this hated crime at the very peak of the international judicial scene. Taking into account the circumstances which were specific to each case, the three applications also invoked various violations of international law relating to the principle of the prohibition of the use of force, the principle of non-intervention, international humanitarian law, international protection of human rights or international environmental law.

In the same manner the motion to institute proceedings filed by Bosnia and Herzegovina, that of Yugoslavia included a request for the indication of provisional measures

[16] Resolution 2171 (2014), United Nations document S/RES/2171 (United Nations Security Council, 21 August 2014), para. 18–19.

[17] "Report of the Advisory Group of Experts for the 2015 Review of the United Nations Peacebuilding Architecture (2015) ", para. 46.

[18] The "palava hut" represents an indigenous reconciliatory and non-adversarial process of justice and conflict transformation used to resolve dispute relating to such issues as divorce, land, theft, and occasionally murder and rape by many ethnic groupings in rural Liberia.

[19] "From Conflict Resolution to Prevention: Connecting Peace Huts to the Police in Liberia", UN Women, the September 19, 2012, http://www.unwomen.org/en/news/ stories / 2012/9 / from-conflict-resolution-to-preventionconnecting-peace-huts-to-the-police-in-liberia.

[20] These efforts could be reinforced by the presence Women in the High Level "Human Rights First" Advisory Group.

[21] The international Court of Justice hereinafter "ICJ".

[22] The North Atlantic Treaty Organization hereinafter "NATO".

[23] The *Rambouillet Agreement* was a proposed peace agreement between the Federal Republic of Yugoslavia and a delegation representing the Albanian majority population of Kosovo. It was drafted by NATO and named for the *Château de Rambouillet*, where it was initially proposed in early 1999. The agreement is significant because of the fact that Yugoslavia refused to accept it; thusly, NATO used the Yugoslavian refusal as justification to start its intervention in the Kosovo War. Belgrade's rejection was based on the argument that the agreement contained provisions for Kosovo's autonomy that went further than the Serbian and Yugoslav governments deemed as reasonable.

[24] The Convention on the Prevention and Punishment of the Crime of Genocide of December 9, 1948 hereinafter, the Genocide Convention.

invoking the urgency of the situation and the risk of escalations. Yugoslavia thus asked the Court to indicate that each state challenged by it must "immediately cease to use the use of force and (...) refrain from any act constituting a threat of recourse or a use of force against the Federal Republic of Yugoslavia"[25].

Divided by the principle of the consent of the parties to establish its jurisdiction[26], the Court assessed the scope of this principle in the present case in order to decide that it did not have *prima facie* jurisdiction in any of the proceedings. It could therefore not enforce orders for provisional measures.

The argument was that of its *lack of jurisdiction*[27] and the *justiciability of the disputes* was in no way called into question: the disputes were political, but they were also legal and were liable to be subject to judicial review.

In nuce, the limits to the intervention of the International Court of Justice is the principle of the consent of the parties.

The requests for provisional measures were based on different credentials. If each of the ten applications purported to base the jurisdiction of the Court on Article IX of the Genocide Convention[28], Yugoslavia, having deposited a declaration of recognition of jurisdiction on the basis of Article 36, paragraph 2 of the Statute of the Court on April 25, 1999, also attempted to take advantage of the declarations made in the application of this article by Belgium, Canada, Spain, the Netherlands, Portugal and the United Kingdom. It also invoked Article 38, paragraph 5 of the Regulation[29] in respect of Germany, the United States, France and Italy. In addition, Yugoslavia invoked the Convention of Conciliation, Judicial Settlement and Arbitration of March 25, 1930, concluded between Belgium and the Kingdom of Yugoslavia, as well as the Treaty of Judicial Settlement, Arbitration and Conciliation, of March 11, 1931, between the Netherlands and the Kingdom of Yugoslavia.

The Court did not order provisional measures, considering that it did not *have prima facie jurisdiction*. For the court, the *veil* of the appearance of jurisdiction with which it had draped certain previous cases was not sufficient in this case. It did not therefore find it useful to deal with the other conditions relating to the decision to enforce or not orders for

[25] Case relating to the lawfulness of the use of force (Yugoslavia v. Belgium), para. 15 of the Ordinance on the request for provisional measures (hereinafter "the Ordinance"). For ease of reading, references to Court orders will be taken from the decision in respect of Belgium, unless the problem addressed is specifically addressed only against another part. All the orders and pleadings can be consulted on the C.I.J.'s website: www.icj-cij.org

[26] Principle reaffirmed in the judgment of 30 June 1995 on East Timor (Portugal v. Australia), C.I.J. Rec. 1995, p. 101, para. 26: "The Court will recall in this regard that one of the fundamental principles of its Statute is that it cannot settle a dispute between States without the latter having consented to its jurisdiction (...)"

[27] Consider paragraphs 45 and 46 of the order; para. 45: "Considering that the Court has concluded above that it had *prima facie jurisdiction* to entertain the request of Yugoslavia neither on the basis of article 36, paragraph 2, of the Statute, nor on that of article IX of the Genocide Convention; and that it considered that it could not, at this stage of the procedure, take into consideration the additional basis of jurisdiction invoked by Yugoslavia; (...); para. 46: "Considering, however, that the conclusions reached by the Court in these proceedings in no way prejudge the jurisdiction of the Court to hear the merits of the case, or any question relating to the admissibility of the application or the merits itself, and that they leave intact the right of the Yugoslav Government and the Belgian Government to assert their means in the matter."

[28] Article IX of the Genocide Convention reads as follows: "The differences between the Contracting Parties relating to the interpretation, application or execution of this Convention, including those relating to the responsibility of a State for genocide or any of the other acts listed in article III, will be submitted to the International Court of Justice, at the request of a Party to the dispute".

[29] Article 38 (5) of the Regulation reads as follows: "When the applicant intends to base the jurisdiction of the Court on consent not yet given or manifested by the State against which the request is made, the request is transmitted to that State. However, it is not included in the general role of the Court and no procedural act is carried out as long as the State against which the application is made has not accepted the jurisdiction of the Court for the purposes of the case."

provisional measures, in particular having regard to the situation and its urgency. While adopting this position, it nevertheless showed that it was sensitive to these aspects.

It did so, by noting its *obiter dicta* calling for the respect of the principles and norms of international law.

The Court was thus able to face the predicament of many judges who wanted the Court not to remain silent in the context of a dispute emphasizing important questions in reference to the international legal system. Judge Higgins' words are revealing in this respect: "Finally it should not be thought that the Court, because it has had to address the question of its prima facie jurisdiction in the case brought by the Federal Republic of Yugoslavia, is indifferent to the great suffering in Kosovo and Yugoslavia. Indeed, the preambular paragraphs of its Order show otherwise. (...)"[30].

Using a vocabulary carefully chosen and attentively weighed to reflect the different positions of the judges, the fundamental principles of international law relating to the maintenance of international peace and security are set out, emphasizing the importance of respecting the obligations of the Charter, as well as the rules of international humanitarian law. It should also be noted that the wording of some of the *obiter dicta* is not very different from that of measures ordered by the Court, in particular in Nicaragua v. United States[31]: in fact, the ICJ had then asked the two parties, by way of provisional measures, not to aggravate the dispute. This formula has been used since then in various other cases. In addition, the role of the Security Council is discussed, albeit in the form of indicia, to remind it of its responsibilities under Chapter VII of the Charter.

If Yugoslavia has brought its disputes before the Court within the framework of the Genocide Convention, it was undoubtedly primarily to benefit from an arbitration clause which would establish the jurisdiction of the judicial organ. To do so, it argued that the air strikes constituted violations of the Convention. The Court's response was that of a brief and final appeal to the definition of the crime of genocide, and to its *prima facie* non-application to the cases before it. The Court retained eight cases on its role under the 1948 Convention; however, it is very unlikely that the Court will diverge from its interpretation of the concept when the cases come to the merits. Another trend is that of "securing" international relations by means of strengthening the role of international actors. The impact of the Balkan war and the conflict in Kosovo are also being felt in this area. We only have to see directions in the European and pan-European spheres, whether it be the European Union or NATO.

The European Union

Crisis management operations and missions were indeed introduced into the Union Treaty, as an EU competence, only by the Treaty of Amsterdam which offers a first definition widely used, that however has some variants, to the Western European Union[32] system. Thus Article 17(2) proposed a first definition of the scope of the *Petersberg missions*[33] that the EU is authorized to develop. These are 4 categories of external operations: humanitarian and evacuation missions, conflict-prevention and peacekeeping missions, combat force missions in crisis management, including peacekeeping, missions for post-combat stabilization and

[30] Lawfulness of the use of force (Yugoslavia v. Belgium), separate opinion of Judge Higgins, para. 30.

[31] Military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America) - Provisional Measures, Order of May 10, 1984, ICJ Rec. 1984, pp. 169.

[32] WEU was created by the Treaty on Economic, Social and Cultural Collaboration and Collective Self-Defense signed at Brussels on 17 March 1948 (the Brussels Treaty), as amended by the Protocol signed at Paris on 23 October 1954, which modified and completed it.

[33] These missions were set out in the Petersberg Declaration adopted at the Ministerial Council of the Western European Union (WEU) in June 1992. On that occasion, the WEU member countries declared their readiness to make available to the WEU, but also to NATO and the EU, military units from the whole spectrum of their conventional armed forces.

assistance. At that time, they were often described as *Petersberg missions* in reference to the WEU missions and operations which this organization decided in 1992 to adopt in response to the new context created by the fall of communism.

The Lisbon Treaty on the EU (TEU) has perfected the institutional framework aimed at increasing the EUs' responsiveness to situations outside European borders, raising the effectiveness of the means available for promoting peace and security. Article 42(1) specifies that the tasks that the Union develops in order to carry out within the framework of its Common Security and Defence Policy (CSDP)[34], namely peacekeeping, conflict prevention and strengthening international security, in accordance with the principles of the UN Charter, are missions the *shall be undertaken using capabilities provided by the Member States*. It further states that the CSDP *shall include the progressive framing of a common Union defence policy*. Pursuant to articles 42(5) and 44, the treaty provides that the Council can entrust the accomplishment of a mission to a group of states if they so desire and have the necessary capacities; in this particular case, it is these States which, in association with the High Representative, agree among themselves on the management of the mission and regularly inform the Council of its completion.

The promotion of human rights and the European Golden Standard in Human rights constitutes the highest threshold in crises management in the European context. To better understand the role that the European Court of Human Rights when called upon to play a role in crisis assessment and management, it is useful to take a step back and take a broader look at the concept of crisis and the place it occupies in contemporary societies.

The judgments of the European Court of Human Rights which deal with the concept of crisis and risk management number in the hundreds.[35] It is therefore not possible to paint a precise and detailed portrait of how the concept is treated by this abundant case law. The subjects concerned are also very numerous, even if it appears that the issues related to Articles 2, 3 and 8 are predominant[36]. In the following lines, we will focus on the issues most commonly addressed by the Court, with the ambition to modestly outline some trends that emerge from a first examination of the mass of decisions available.

In the field of the European Convention on Human Rights, one could start from the idea that any situation which entails a violation of a right necessarily corresponds to serious prejudice. In numerous cases relating to Article 2 for example, the Court did not ask whether, before the death occurred, there was a crisis situation in which the violation of the right to life occurred; the Court limited itself to analyzing, *prima facie,* whether there was a serious crisis that could result in death and whether the state responded appropriately to try to prevent such situation. In other words, the assessment of gravity cannot directly concern the question of the violation of the Convention, which will only be decided after the judgment of the Court.

We have to mention the ECHR in the context of the Copenhagen requirements, that all states are members of the Convention and that it has infused the normative system Europe, promoting democracy through human rights.

Thanks to the Copenhagen criteria, we could shape the reforms of the EU states and thus the political, economic and social reconstruction of the candidate countries. Thus the EU imposes on its candidates, formerly subjected to a totalitarian regime, high democratic standards: promotion of gender equality, recognition of minorities, end of the death penalty,

[34] The Common Defense and Security Policy hereinafter "CDSP".

[35] As far as we can consider that this is a relevant quantitative index, we note that on March 31, 2019, the introduction of the word "risk" and "crisis" in the search engine "Hudoc" of the European Court of Human Rights showed over 3,000 results among the substantive judgments delivered by a chamber or the Grand Chamber of the Court.

[36] In this sense, *see* L. Seminara, *"Risk Regulation and the European Convention on Human Rights",* European Journal of Risk Regulation, 2016, pp. 733-734.

end of torture, recognition of international institutions and respect for the environment. Turkey, through its judicial reforms and the recognition of the Kurdish community, was a model of goodwill for integration; Likewise, Croatia, finally joining the EU, has agreed to cooperate with the International Tribunal to turn the page on the Balkan war following the dismantling of Yugoslavia. The EU's "soft power" instruments, embodied by the Copenhagen criteria, can boast of having exported its democratic model, a dynamic of solid development and, above all, peace on a continent so often torn apart. The EU has received the Nobel Peace Prize in 2012 for all of its actions in favor of "peace and reconciliation, democracy and human rights in Europe." Thus, the enlargement policy conditioned by the Copenhagen criteria was the most effective foreign policy of the Union.

However, it should be noted that this "soft power" instrument necessarily remains limited to the candidate countries for the EU, those which are ready to comply with this exercise in convergence. As soon as the number of candidate countries is reduced (either because they have been already integrated or because the attractiveness of the EU is decreasing for certain states) the strength of the Copenhagen criteria disappears.

The progressive development of human rights is intrinsically linked to the desire to create an environment based on the values of representative democracy, perhaps the greatest legacy Europe has brought humanity.

To conclude our scientific enquiry, we must highlight that *institutionalism*, as the palimpsest that has stored, filtered and rendered the knowledge to effectively promote peace and security is one of the main guarantees of employing crisis management as a continuous process.

Crisis management is not a concept liked solely to security or international relations, but to organizational theory as well, and the approach must be employed by all institutions alike, whether public of private.

The *institutionalist* and *neo-institutionalist* literature has written extensively on the integrationist effects of international organizations and how the moral authority enjoyed by such institutions has the effect of infusing the international milleu with the necessary tools for the promotion of peace and security in a comprehensive approach. The crisis management continuum must be understood as a sum of actions directed at the maintenance of stable peace and the promotion of the highest standards in human rights. The activity of all international actors, especially international organizations and jurisdictions, acts as a permanent guardian and protector, collecting *lessons* and evening out discrepancies when necessary. Peace and stability are maintained in equilibrium only through crisis management.

We would like to strenuously point out that the importance of the Organization for Security and Cooperation in Europe was not overlooked, it was purposely and surgically excised in view of a further and elaborate future study to be conducted by the authors.

BIBLIOGRAPHY

1. ****Fragile and Conflict-Affected States: Signs of Progress to the Millennium Development Goals,* la Banque mondiale, le 2 mai 2013, http://www.worldbank.org/en/news/press-release/2013/05/02/fragile-and-conflictaffected-states-signs-of-progress-to-the-millenniumdevelopment-goals.
2. ***Resolution 2171 (2014), United Nations document S/RES/2171 (United Nations Security Council, 21 August 2014), para. 18–19.
3. ****The Challenge of Sustaining Peace*, Document de l'ONU A/69/968–S/2015/490 (Groupe consultatif d'experts pour l'Examen 2015 du dispositif de consolidation de la paix des Nations Unies, le 29 juin 2015), § 24 ; « State of the World's Mothers 2014: Saving Mothers and Children in Humanitarian Crises » (Save the Children, 2014).

4. *** UN Security Council, Security Council resolution 1325 (2000) [on women and peace and security], 31 October 2000, S/RES/1325 (2000).
5. ***Uniting Our Strengths for Peace - Politics, Partnership and People, UN Document A / 70/95 – S / 2015/446 (Independent high-level group to review United Nations peace operations, 16 June 2015), para. 62
6. Coman, R.*, Why and how do think tanks expand their networks in times of crisis? The case of Bruegel and the Centre for European Policy Studies,* Journal of European Public Policy, Taylor & Francis Online Review, 2018 .
7. Cox, R.H. and Béland, D., *Valence, policy ideas and the rise of sustainabilit*y, *Governance* 26(2), 2012, pp. 307–28.
8. Ruby, Felicity, *Security Council Resolution 1325: A Tool for Conflict Prevention?*, *in* Rethinking Peacekeeping, Gender Equality and Collective Security, 2014, p. 182.
9. Seadbrook, Leonard, Tsingou, Eleni, *Europe's fast- and slow-burning crises,* Journal of European Public policy, vol. 26, Issue no. 3, 2019.

WOMEN IN THE INTERNATIONAL ARENA. WITNESSES OR ARCHITECTS?

Elena-Loredana FLORESCU
International Relations Student, University of Bucharest, Faculty of Political Science
Architecture Student, “Ion Mincu” University of Architecture and Urbanism
elenaloredanaflorescu@gmail.com

Abstract: *In the global context of the process of increasing gender equality, international relations are adapting to the new dynamic of the inclusive system that is slowly, but steadily becoming the new reference point. In the complexity of the various stages that women had been through until this point, their role shifted continously from being a stander-by to being an active participant in the design of international events, a role which is now established as one that is equally viable for both men and women.*

Keywords: *gender equality, international relations, conflict.*

Introduction

International relations, until now, had been taking the experiences of men and women about the state for granted, disregarding that the experiences are varying according to each gender, inside and outside the border of the state. The states being in a continuous change, the process of globalisation and fragmentation are weakening the state from above and beyond, thus, states, sovereignty and international relations require an adaptive thinking in order to respect the global dynamics and gender relations seriously.

Gender differentiation, among with ethnicity, exceeds other socially defined attributes such as class and nationality, because of their quality of being beyond our capability to manipulate or change them. Therefore, being a woman is a permanent determinant in conducting relationships in societies that most of them continue to be patriarchal.

Whether we discuss about contemporary situations or history, women’s status in the society represent an active and still developing bias. They represent that part of the society that is seen as being prised but defenceless, valued but abused, crucial yet overlooked. The role that women had in society, their part in the changing of events, had been often neglected throughout the history in the textbooks and stories that are commonly known. Their contribution in the international events is often unnoticed in comparison to the ones of men, in what was described as being "a man’s world”. Because of the unnequal access to power and favorable circumstances, women tended to engage in strategies that were adressing the distribution of positions in the hierarchical structure of power. [1]

A conflict in the international arena is ”*a dynamic phenomenon structured on phases or succesive stages, identifiable according to its evolution; the gradual phasing out of the conflict is clearly linked to the feedback of stakeholders involved in awareness, perception, and interpretation of favouring, enhancers factors.”*[2]. The dynamic of the conflict can also be presented in the form of a house: the house per se represents just a part of the problem, while

[1] Abedin, S. M. , ”Women in search of equality, development and peace: a critical analysis of the platform for action, fourth world conference on women, and the Islamic perspective”, Journal of Muslim Minority Affairs, volume 16, 1996, pp. 73-98

[2] Toma Plesanu, Dorin-Valeriu Badulescu, „A new approach to the life cycle of the conflict”, “Proceedings/ The 14th International Scientific Conference “Strategies XXI”/Strategic changes in security and international relations”, Volume 2, “Carol I” National Defence University Publishing House, 2019, pp. 26-32

its foundation structure represents the part of the conflict that is not visible. The house concludes the general data of the conflict, the observable attitude, the evidence, while the foundation that is hidden from the eye, in the underground, represents the motives of the parties involved, the tension that led to its eruption, the feelings gathered through time. But how can women find their place in the construction or the destruction of the conflict house?

Paving the road to equality, by women for women

The main points of interest in the study of international relations are states and sovereignty. In trying to understand the way that we, as a population, organise politically, states continue to monopolise our defying term, therefore this is the reason that people identify themselves as being American, Chinese or Russian. Some of the critiques believe that the state, along with citizenship, could be considered gendered. The question asked is according to what the "body politic" becomes associated with male bodies, and the reason why women are finding it so hard to become a full citizen of their state. One of the explanations of this is the fact that the state lays its high politics mostly in its military and security concerns, which are fully associated with men, and in its foreign policy.[3]

Having this in mind, is more notable that, since the classical democracy in Ancient Greece, women did not have a chance to actively participate in the development of the *polis*[4], as they were not considered to be a citizen of it. In order to be a citizen and have a role in the direct participation of the polis, you needed to be, firstly, a man. Therefore, since the beginning of the early democracies women were assumed the roles of witnesses, not being able to have a say in the decision-making groups.

During the Roman Empire, women were enjoying considerable social flexibility due to the Etruscan and Hellenistic ideas. Due to the Private Law[5], they were able to gradually achieve independence at a larger extent than the women from Ancient Greece, but they where still excluded from all the participation in public affairs, whether as voters, senators or magistrates. The only exceptions were priesthoods, where they could be accepted as Vestal Virgins. Therefore, their citizen status was still denied, their participation in politics and public affairs not accepted. The answer about their general involvement in the public life is only through men, by counselling (when their opinion was required), cajolement, manipulation or, sometimes, manipulation.

Their activity remained behind the scenes, as it is also portrayed by Even Tanaquil, the prototype of woman of character and determination who leaves a lasting mark on the political field. Even Tanaquil was from a powerful Etruscan family in Tarquinii, Etruria. The only thing that she was able to do was to make her husband, the son of an immigrant, who could not be able to gain power in Tarquinii, the Etruscan king of Rome, and Servius Tullius, her protégé, his successor. Even with this degree of intervention in politics, an intervention which would not had happened if she was able to become a queen herself, people criticized it.[6]

In the early modern Europe, political histories are characterized by being focused on generations of men: one king follows another in succesion, from fathers to sons and grandsons, brothers and nephews. England is one example of this practice, with over 200 years of patriarchal power structures, from Edward III to Henry VIII and Edward VI. After

[3] Jan Jindy Pettman, "Worlding Women: A feminist international politics", Routlege, 1996, pp. 12-20.

[4] Transliteration of the Greek word for "city-state". In Plato and especially Aristotle, *polis* has the normative connotation of the best form of social organization. –"Oxford/ Concise Dictionary of Politics and International Relations".

[5] Rafael Domingo, ICS Professor of Law, University of Navarra - "Roman Law: Basic Legal Concepts and Values", SSRN Electronic Journal, January 2017, pp. 7-12.

[6] Richard A. Bauman, "Women and Politics in Ancient Rome", Routlege, 2003, pp. 1-12.

the death of Edward VI, something interrupts the usual development when he is succeeded at the throne by his sister, Mary.

The idea of a women on the throne of England was terrifying to many, John Knox, the Protestant reformer, being among them. In his writing, "The First Blast of the Trumpet against the Monstrous Regiment of Women", he states that *"to promote a woman to bear rule, superiority, dominion, or empire above any realm, nation, or city is repugnant to nature," an "insult to God, and a "subversion" of order, equity, and justice, and since he concluded that rule by women is the "most detestable and damnable" of all the "enormities" faced by men"*.[7]

John Knox's argument is constructed as if women had never had a position of power, had never ruled as queens before since biblical times. The plans of the international "house" was in the hands of a woman: establishing the allies, establishing the foreign policy and controlling the institutions of the nation. History was, until then, the result of a long list of men, each of them leaving their legacy behind, for people who were already being used to appreciate, understand and commemorate them. The population was not prepared nor ready to accept immediately the idea of a queen, therefore, serving and recognising her achievements were often left behind or not taken into account.

This dormant state in which women were founding themselves, as being witnesses to history making, started to slowly shift at one point in history that marked an unique event up to that moment: First World War, or, as it was called then, the Great War. The war was met then with a surprisingly enthusiasm due to the raise of nationalism in the decades before. Many young people were inflicted with feeling of greatness towards their countries and men were encouraged to train in militaristic programmes in order to combine their nationalist feelings with the army. Therefore, when the war began, men left everything behind - their jobs and families to fulfil the biggest duty of them all: to defend the country. But what were women left to do? History was again in the hands of men, being in the front line and acknowledging the turn of the events.[8]

The Great War brought to light the ambivalent characteristics of a women: the ability to encourage, to sustain the morale, to empower men to fight the war, but also the adaptability and ambition to take the matter into their hands in the absence of them, to keep the things running at the home front. The governments took advantage of the situation and used it to work its best interests.

Even though feminine characteristics are not universally identical, there are some traits that are considered to be generally available, and propaganda during war knew exactly how to use them in order to extract the results needed. For example, posters used in Britain portrayed a picture of three persons, two women and one child, who seem to be part of the same family, as they are standing in front of the window, gazing at a marching troop of soldiers going to war. The slogan of the poster is: "Women of Britain say- "Go!". In this case, the women, as the ones who are now in charge to take care of the family (as they are portrayed in the poster, with the little child seeking security behind them), were seen as the most important subjects who could encourage the potential recruits to enlist. The slogan suggested that the men had their full support, in order to have their protection assured and that their role was to stay behind.

On the other hand, the raise of enthusiasm towards nationalism did not affect only men: women were prepared to do their part in the on-going conflict. Even if they did not have acces to manage the visible part of the conflict, their activity opperated on a more subtle level,

[7] Sharon L. Jansen, "Debating Women, Politics, and Power in Early Modern Europe", Palgrave Macmillan, 2008, pp. 11-33.

[8] Kathryn J. Atwood, "Women heroes of World War I.16 Remarkable resisters, soldiers, spies and medics", Chicago Review Press, 2014, 12-23.

governments beginning to encourage women to begin public activities in the occupations left vacant by the shortage of men. Volunteer positions in the medical services were taken by women who could afford working without being paid and those who were depended on a source of income would choose to work in munitions factories (usually getting more income than elsewhere), making not only ammunition and weapons but also gear for war that, until then, was not mass-produced, such as binoculars.

Women started to see the opportunities that they would get out of stepping from their home and having a work place. Because they were not considered yet full citizens, without having the right to vote, they realized that their involvement could help them prove that they were worthy of possesing a full citizenship. But, after the end of the war, women soon realised that they were not having any notion of how could they control the extent of their services. In fact, in the period before the end of the war, the idea that working mothers might affect the psychology of their children placed in daycare started to be implemented. In this way, women could understand the message that their role, already in the shadow, in the run of the events is just temporar and that the pre-war family structure needs to take its place back, once the war is over.

After the Great War, in the wake of the disscusion about equal gender rights, many women started to feel that their role in the society could evolve. An example of women starting to be accepted in meddling in conflict mediation after the Great War is Queen Marie of Romania. Because of the differences of opinion between the Romanian Prime Minister of that time, Ion I.C. Bratianu and the French Prime Minister Georges Clemenceau, the romanian delegation had to leave, Queen Marie was sent to the Paris Peace Conference instead, hoping to solve the situation. Using her diplomatic intelligence, she conducted the negotiations herself, without the help of the ministers that were accompanying her. When leaving Paris, she managed to obtain for her country supplies and, later that year, Greater Romania gained recognition, therefore its territory doubled and population increased. [9] Queen Marie was given the chance to act upon not only the visible part of the situation, but also to the hidden one, firstly knowing how to communicate with Georges Clemenceau in order to change its perception about the romanian delegation and secondly using her charismatic qualities to attract the people's support.

During the Second World War, a women's phenomenon was happening in the world. After the inter-war period of countries acknowledging women's right to vote, it was their time to take an active part in the conflict and pursue their national duties, being equal to men. Women served in many countries taking part in the war, of which are listed: 225,000 in the British army, 450,000 to 500,000 in the United States' army, 500,000 in German army and about a million in the Soviet army.[10] The American women formed the Women's Army Corps, the members being the first women that had another occupation than being a nurse who served in the army during war.

Because of the opportunity to offer their contribution, women took part in all the military specialties, even those considered to be the most “masculine” ones. Many nations were still not ready to get accustomed to the idea of a woman in uniform. A lot of linguistic problems also occurred, because there was no feminine gender for the words describing different war positions, because until then, there were no women to do that work, such as: “machine gunner” or “tank driver”. Nonetheless, the need for working hands was increasing,

[9] https://www.romaniaregala.ro/jurnal/regina-maria-incepea-acum-99-de-ani-legendara-sa-vizita-in-franta/ accessed on 5.03.2020

[10] Svetlana Alexievich, “The unwomanly face of war/An oral history of women in World War II”, Random House New York, 2017, p. 7.

therefore the political and military leaders realized that women could supply the in the military and industrial sectors. [11]

Conclusion

A century apart since women gained the right to vote, they became more and more active in electoral or party politics and social movements, campaigning for education reforms, public health and child welfare. The need of women to actively participate in the public affairs, not just for a representative polity but also for the qualities that they bring to the diplomatic community was acknowledged and required.

The United Nations' Development Programme (UNDP), within the United Nations system, focused their 2030 Agenda for Sustainable Development on gender equality. The Gender Equality Strategy 2018-2021 was adopted by UNDP, which "*commits the organization to intensify its efforts to mainstream gender equality across all of its areas of work".*[12] This strategy addresses the removal of structural barriers that constrained the empowering of women's economic growth and promoted women in the decision-making positions.

The share of women in decision-making positions raised considerably, from women being in the position of the leader of the United States' diplomacy (Madeleine Albright) to women being in the position of being the Prime Minister of England (Margaret Thatcher). Even if in 2019, in the European parliaments of the EU member countries, women accounted for 31% of its members[13], the challenges that they have to face are bigger than those that occur to men, due to the still existing stereotypes, biases and lack of support for women to pursue careers. According to the Global Gender Cap Report 2020, it will take almost a century from now for women to become truly equal to men in Europe, although the European Union, among its history, was the biggest advocate for women's rights.

Gender equality represents, in the end, a fundamental human right. The process of women regaining their power should be one from which both genders should thrive upon, because it helps the society to develop not only socially, by respecting and supporting women in their activities, which leads to healthier families, but also economically, due to the increase of jobs and therefore money income. Women have the right to design not only their lives, but also help in designing the international arena, enhancing diplomacy with their intuition, sensibility and courage.

BIBLIOGRAPHY:

1. Abedin, S. M. , "Women in search of equality, development and peace: a critical analysis of the platform for action, fourth world conference on women, and the Islamic perspective", Journal of Muslim Minority Affairs, volume 16, 1996.
2. Toma Plesanu, Dorin-Valeriu Badulescu, „A new approach to the life cycle of the conflict", "Proceedings/The 14th International Scientific Conference "Strategies XXI"/Strategic changes in security and international relations", Volume 2, "Carol I" National Defence University Publishing House, 2019.
3. Jan Jindy Pettman, "Worlding Women: A feminist international politics", Routlege, 1996.
4. Rafael Domingo, ICS Professor of Law, University of Navarra - "Roman Law: Basic Legal Concepts and Values", SSRN Electronic Journal, January 2017.

[11] Judith A. Bellafaire, "The Women's Army Corps", CMH Publication, 2005, pp. 4-29.

[12] https://www.undp.org/content/undp/en/home/2030-agenda-for-sustainable-development/people/gender-equality.html , accessed on 9.03.2020.

[13] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/gender-equality/gender-balance-decision-making-positions_en, accessed on 9.03.2020.

5. Richard A. Bauman, “Women and Politics in Ancient Rome”, Routlege, 2003, pages 1-12
6. Sharon L. Jansen, “Debating Women, Politics, and Power in Early Modern Europe”, Palgrave Macmillan, 2008.
7. Kathryn J. Atwood, “Women heroes of World War I.16 Remarkable resisters, soldiers, spies and medics”, Chicago Review Press, 2014.
8. https://www.romaniaregala.ro/jurnal/regina-maria-incepea-acum-99-de-ani-legendara-sa-vizita-in-franta/ accessed on 5.03.2020.
9. Svetlana Alexievich, “The unwomanly face of war/ An oral history of women in World War II”, Random House New York, 2017.
10. Judith A. Bellafaire, “The Women’s Army Corps”, CMH Publication, 2005, pages 4-29
11. https://www.undp.org/content/undp/en/home/2030-agenda-for-sustainable-development/people/gender-equality.html, accessed on 9.03.2020
12. https://ec.europa.eu/info/policies/justice-and-fundamental-rights/gender-equality/gender-balance-decision-making-positions_en, accessed on 9.03.2020

DYNAMICS AND OPERATIONAL ENGAGEMENT OF THE EUROPEAN UNION IN MANAGING THE CRISES AND CONFLICTS IN NORTHERN AND EASTERN PARTS OF AFRICA

Marian Iulian COJOCARU
Ph.D. Student, National Defence University "CAROL I"
iulicojocaru@yahoo.com

Dumitru Cătălin BURSUC
Navy Captain, Professor, Ph.D., National Defence University "CAROL I"
catalin258@yahoo.com

Abstract: *Africa where? It is a question whose answer can be extracted from the current components of the continent's life. At present, Africa has a population of over two hundred million people, with the possibility of doubling it by 2050. The demographic increase is supported by the youth of its inhabitants with an average age of just over 17 years. The increase of the average life span from 35-37 years to 43-46 years is the premise of a dynamic development as more and more countries emerge under the overwhelming burden of dictatorships, secret police and tribal paternalism. It is imperative that the European Union remain strong and supportive, even after the departure of the United Kingdom, share a common vision and, above all, act together. Based on these considerations, the new European Union Global Strategy for the Foreign Policy and Security was formulated, being focused on five major priorities: Union security, the resilience of states and societies in the east and south of the Union, an integrated approach to conflicts, regional order based on cooperation and global governance for the 21st century. Starting from these considerations, a number of questions have arisen: "Where is Africa in the whole global geopolitical game?" "How important is the control of this continent for the preservation or change of the world order?" In all its diversity, Africa is increasingly present on the international stage, being more confident, more dynamic and more optimistic than it has ever been. In the last two decades, Africa has shown impressive economic progress, with positive changes in several countries. An increasing number of African regional governments and organizations are taking the lead in addressing security, policy and poverty reduction challenges within and beyond their borders and playing a more active role in promoting good governance and the rule of law.*

Keywords: *diversity, conflicts, reorientations, employment, operations, missions.*

1. Africa in the current context of the evolution of the security situation

The mix of European cultures is a daily challenge that represents the main strength: diversity is what gives power to the Union. In recent times, the existence of the European Union is increasingly being questioned, and the situation, in general, has become more unstable and uncertain. The last years have represented a difficult period which has been deepened by the desire of the citizens of Great Britain to leave the European Union, a desire expressed during the referendum of 2016. The experts in the field appreciated that Brexit aftermath may have a domino effect over other countries and it must be admitted that the British vote has put Europe at serious trial.

Although African leaders feared the collapse of communism in European countries and that this would lead to a decreasing interest in the development of their countries, the evolution of events and directions of collaboration with the outside world have expanded and new goals and reorientations have emerged. The result of these reorientations made the European Union the main partner of Africa. Africa was regarded by geopolitics as Freidrich Ratzel, Rudolf Kjellen or Nicholas Spykman, as a mysterious territory, placed outside significant planetary events, being treated arbitrarily and unfairly as the outer edge of the periphery of human society.

We live in a difficult world, which is increasingly contested, ever more connected, but also more complex, taking into account our common interests, principles and priorities. The European Union is primarily based on the values engaged in the Treaties and must make the most of its strengths and historical achievements, but the most important thing at present is that the member countries remain united in maintaining a truly strong Union, which will play its role of global actor in the world. However, this difficult period can be an extraordinary opportunity. Global economic growth, mobility and technological advancement, together with deepening partnerships, allow us to thrive and offer the possibility of more and more people to escape poverty and live a better and freer life. There is hope that the European Union will continue to exist, promote peace and guarantee the security of its territory and its citizens. Internal and external security are increasingly interdependent: peace at home depends on peace across borders, and this implies the achievement of the objectives of the new Security Strategy. This is why the European Union has chosen to "*extend the shield of protection*" so far to defend its territory.

Also, a united and prosperous European Union depends on an open international economic system and sustainable access to global common goods. "*Technological developments, the ability of digital communication to unite remote geographical areas, but with common or close interests, the increasing demand for raw materials useful to the new computer industries, rare in the world and abundant in Africa, have made this continent a proximity territory also due to more and more diverse relationships*".[1]

2. Operations and missions of the European Union in the Northern and Eastern parts of Africa – developing the story

The European Union, through its foreign, security and defence policy can act globally as an entity. Through this policy, the member states can face the challenges that they cannot solve on their own, thus contributing to the security and prosperity of European citizens. "*The policy is implemented by the head of the EU's foreign affairs, the High Representative of the Union for Foreign Affairs and Security Policy (who is also Vice-President of the Commission) and by the European External Action Service, the EU's diplomatic service.*"[2]

The European Union will continue to promote a global order based on rules, whose fundamental principle will be multilateralism and the United Nations. There is a major interest in promoting agreed rules to provide global public goods and to contribute to a peaceful and sustainable world. "*At present, the European Union is fully committed to developing a global profile in the international security architecture, benefiting from a strategic vision, integrated within its own Security Strategy, as well as the tools needed to assume an operational role in the field of crisis management*."[3]

Overall, the Common Security and Defence Policy has become an important tool within the European Union's external action mechanism, and its operations are the most visible manifestations of EU activity in fragile states. However, in recent years, a number of challenges have emerged that show the limits of what the European Union and its Member States are capable and willing to do for a safer world.

The effectiveness and impact of CSDP operations require a strategic objective and coherence between the different components of the European Union's External Action. A joint communication by the European Commission and the HR/VP on the "*global approach to external conflicts and external crises*" defined the global approach as an ambition to make the European Union's external action more coherent, efficient and strategic by "*capitalizing on*

[1] Nicolae Melinescu, *Vecina mea, Africa*, Editura Cetatea de Scaun, Târgoviște, 2018, p. 8.

[2] https://publications.europa.eu/ro/publication-detail/-/publication/ accessed 11.03.2020.

[3] Politica Europeană de securitate şi apărare/Departamentul pentru integrare euroatlantică şi politica de apărare/scurt istoric.

the entire range of tools and resources."[4] In practice, the component of the Common Security and Defence Policy is in fact a comprehensive approach that involves increased coordination within a PSAC operation, as well as between a PSAC operation and other EU actors, such as Member States, the European Union delegation and the European Commission on the site.

In the case of the military operations, civil-military interaction is a key element. However, the comprehensive approach is more an orientation or a process than an end goal itself. Political, cultural, administrative and even personality-related obstacles are likely to act as inherent constraints on its full implementation.

Lately, progress has been visible in different areas, and the European Union's policy in the field of Common Security and Defence Policy (PSAC) has begun to be much better integrated since 2016. Recent developments, such as increased Commission staff participation in planning and the working groups related to the CSDP, the socialization process between the military and civilian personnel within the European External Action Service (EEAS), the mutual recognition of the links between security and development and the development of regional strategies have contributed, to some extent, to the formation of a culture of coordination that cannot be compared with those that existed many years ago, when the first operations were set up under the aegis of the Foreign Security and Defence Policy (FSDP).

In the process of establishing a PSAC mission, a number of institutions are employed: "*The operations and missions of the PSAC are formally created by the Council of Ministers of the European Union or the Council of the European Union, usually within the Council of Foreign Affairs, which decides unanimously (with the exception of Denmark which has the option to renounce on different issues that will be debated and which have implications in the field of defence). The Council of the European Union defines and implements the EU's foreign and security policy on the basis of guidelines set by the European Council. It also includes EU humanitarian and development aid, defence and trade. The Council, together with the High Representative of the Union for Foreign Affairs and Security Policy, ensures the unity, coherence and effectiveness of the EU's external action.*

The Council of the European Union draws up annually, based on the conclusions of the European Council, guidelines and recommendations for the Member States on EU foreign and security policy".[5]

The creation and development of a CSDP action is the result of a well-defined process, which combines a political assessment of the situation, different planning stages and decision-making procedures. This process is the responsibility of the Council of the European Union and the High Representative and is carried out in accordance with the crisis management procedures, which were revised in 2013. Although the specific procedures are similar for both military operations and civilian missions, there are some variations regarding certain aspects. To trigger a CSDP operation, an immediate response to any type of problem should not be considered, but only as a possible option, along with other political alternatives, such as, among others, diplomatic or humanitarian action, restrictive measures (sanctions) or non-participation.

In ideal circumstances, in the first phase, the European Union assesses whether the CSDP route is the most appropriate to intervene in a given situation. This exercise/phase can be carried out through a process called "*Political framework for addressing crises by the EEAS - European External Action Service, but it is not a prerequisite for triggering a CSDP action*".[6]

[4] https://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_ro_version accessed 11.03.2020.
[5] *The EU and the world: Players and policies post-Lisbon,* a Handbook Edited by Antonoi Missiroli, European Union Handbook, format pdf, p. 52.
[6] *Ibidem,* pp. 52-53.

The Council of the European Union, together with the High Representative of the Union for Foreign Affairs and Security Policy, ensures the unity, coherence and effectiveness of the EU's external action. "*If the Council of the European Union decides that a CSDP operation is the way forward, certain military and civilian entities of the European External Action Service (EEAS) will plan the operation / mission under the authority of the Political and Security Committee (PSC). Planning defines the objectives, mode of operation and assets required for a CSDP operation. The planning process takes place at two different levels, strategically and operationally. At the strategic level, the main planning document is the Crisis Management Concept, which analyses and proposes different political and strategic options of the PSAC, before the creation of the operation. It is produced by the Crisis Management and Planning Directorate (CMPD) of the European External Action Service, in consultation with the military personnel of the European Union (EUMS) in the case of military operations and with the Civilian Planning and Management Capacity (CPCC). Conduct Capability) for civilian missions*".[7]

The concept of Crisis Management is presented by the High Representative for Foreign Affairs and Security Policy to the PSC (Political and Security Committee) and then to the Council, which can approve it and, therefore, formally establish an operation. At this stage, the Council will appoint an operation commander (or the head of the mission for civilian missions - HoM) who will lead the operational phase of mission planning - which involves the elaboration of the Operations Concept - CONOPS - and the Operational Plan - OPLAN. The commander of the operation/Head of Mission leads the process of generating the forces and aims for the Member States to obtain the necessary capabilities to carry out the operation.

At the operational level, planning is carried out differently in the military versus the civilian field. In the military field and in the case of "*major*" operations, planning is carried out by two possible mechanisms. The first mechanism is the European Union's option to use NATO capabilities, in accordance with the agreement "*EU-NATO Berlin Plus 2003*".[8] From this point of view, we would like to point out that only Operation *Althea* in Bosnia corresponds to this option. The second option is to use one of the national headquarters (France, Germany, Greece and Italy) for autonomous operations of the European Union. Due to Brexit, the UK headquarters will no longer be considered. A third option, which has not yet been implemented, is based on the European Union Operations Centre. Smaller non-executive military operations (capacity building and training operations) are commanded/controlled from the theatre and have an element of support in Brussels, without the need to activate an operational headquarters.

In the civil field, missions are planned by the Crisis Management and Planning Directorates - and then by the CPCC (Civilian Planning and Conduct Capability) - which also leads the Civil Planning and Conduct Capability missions. The CPCC director is the head of all civil missions, but each civil mission has a Head of Mission - Head of Mission[9].

The reporting system of civilian missions compared to military operations is slightly different. In military operations, the operation commander reports directly to the European Union Military Committee (EUMC) at regular intervals and may be invited to EUMC and / or Peace and Security Council - PSC meetings, as appropriate. Instead, in civilian missions, the head of all civilian missions (CPCC director - Civilian Planning and Conduct Capability)

[7] *The EU and the world: Players and policies post-Lisbon*, a Handbook Edited by Antonoi Missiroli, European Union Handbook, format pdf, p. 52.

[8] http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/berlinplus_/berlinplus_en.pdf accessed 15.04.2019 - The Berlin Plus Agreement is a short title for a comprehensive package of NATO-EU agreements, based on the conclusions of the Washington NATO Summit.

[9] *Ibidem*.

reports through the High Representative for Foreign Affairs and Security Policy to the Council, as well as to the PSC.

In the context of the general process of consolidating the Common Security and Defence Policy, the European Union continues to refine its concepts and approaches to different areas of interest, adopting, in line with the Comprehensive Approach on External Conflicts and Crises, a series of Regional Strategies. - EU Strategy for the Sahel, Horn of Africa, or the Gulf of Guinea. The Comprehensive Approach aims to make EU action more consistent, more effective, using a strategic approach at the external level. The comprehensive approach involves more than involving in external theatres with civilian missions and military operations, aiming at early engagement in the planning process of an intervention of all the actors that can have added value and facilitating overcoming the crisis (EU Member States, specialized working groups) of the EU Council, EU Delegations from third countries, special EU representatives, diplomatic, civil, military, development assistance and humanitarian actors).

Civilian missions of the European Union in Africa: (EUBAM Libya) - European Union Border Assistance Mission in Libya; (EUCAP Sahel Mali) - European Union Mission in Mali; (EUCAP Sahel Niger) - European Union Mission in Niger; (EUCAP Somalia) - European Union Capacity Building Mission in Somalia. European Union military operations in Africa: EUNAVFOR MED Operation SOPHIA; EUTM RCA – European Union Training Mission in RCA; EUTM Somalia - European Union Training Mission in Somalia; EUTM-Mali – European Union Training Mission in Mali; EU NAVFOR Somalia – Operation *Atalanta*.

The decision of the European Union to plan, conduct and subsequently develop civilian missions or current operations is taken by the EU Member States in the Foreign Affairs Council (FAC). "*Military operations can start after the four planning stages, given that their commanders, military personnel (EUMS), Military Committee (CMUE), Political and Security Committee (CPS) and the Council of the European Union have different roles. The planning stages are: I: Political framework for crisis approach (PFCA) II: The concept of crisis management (CMC) III: Military Strategic Options (MCO, except in CMC) and Military Initiation Directive (IMD) IV: The concept of operations (CONOPS), the Operations Plan (OPLAN) and the Employment Rules (ROE)*"[10].

The cooperation between Africa and the European Union has developed and diversified rapidly. Both, the African Union and the European Union have developed strategies to support and guide each other's cooperation.

The cooperation with the European Union has helped the African Union to have a new and integrated vision, a prosperous and pacifist Africa, led by its own citizens and representing a dynamic force on the global arena.

In order to highlight this topic of the "*European Union operational engagement in North and East Africa*", it can be stated that the international security environment is positively influenced by the processes of European and Euro-Atlantic integration, in fact by the enlargement of the community of the sharing states and promotes the values of democracy and the market economy, in the context of deepening regional cooperation.

In a rapidly changing global security environment, Africa is facing profound economic and political-social changes, and its importance for the internal and external dimensions of Europe's security and prosperity is becoming increasingly evident. Europe and Africa have much to gain from closer political and economic ties, but also much to lose if relations based on close cooperation, stronger, deeper and more action-oriented strategic partnerships are not continued. There are a number of concrete priorities and initiatives for the period 2018-2020

[10] *The EU and the world: Players and policies post-Lisbon a handbook* Edited by Antonio Missiroli, European Union handbook, format pdf, p. 54.

and beyond, which are to be coordinated and strengthened together with EU Member States and refined together with African partners in response to Africa's 2063 Agenda[11] and in line with The overall strategy for the European Union's foreign and security policy.

BIBLIOGRAPHY

1. Nicolae MELINESCU, My Neighbour, Africa, Cetatea de Scaun Publishing House, Târgoviște, 2018;
2. European Security and Defence Policy/Department for Euro-Atlantic Integration and Defence Policy / Short History;
3. *The EU and the world: Players and policemen post-Lisbon* a handbook Edited by Antonio Missiroli, European Union handbook, pdf format;
4. *The EU and the world: players and police post-Lisbon* a handbook Edited by Antonio Missiroli, European Union Handbook, pdf format;
5. African Union, *Agenda 2063*, 2015, https://au.int/agenda2063
6. https://publications.europa.eu/ro/publication-detail/-/publication/
7. https://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_ro_version
8. http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/berlinplus_/berlinplus_en.pdf

[11] *** Uniunea Africană, *Agenda 2063*, 2015, https://au.int/agenda2063 accessed 11.10.2018.

THE NEED FOR THE DEVELOPMENT OF THE NEWEST EUROPEAN GLOBAL STRATEGY FOR FOREIGN POLICY AND SECURITY

Marian Iulian COJOCARU
Ph.D. Student, "Carol I" National Defence University
iulicojocaru@yahoo.com

Dumitru Cătălin BURSUC
Navy Captain, Professor, Ph.D., National Defence University "CAROL I"
catalin258@yahoo.com

Abstract: *Drawing up a new European Union Global Security Strategy started from the premise that the European Union is confronted more and more frequently with a series of major crises, occurring in the interior, but also outside the border area. Given the persistence of a fragile security environment, the High Representative of the European Union for Foreign Affairs and Security Policy and Vice-President of the European Commission, Federica Mogherini, was mandated by the European Council in June 2015 to develop a new European Union Global Security Strategy for foreign policy and security intended to enhance of European, regional and global security. The new European Union Global Security Strategy developed the ambition of a European Union autonomy, and this was so necessary for the promotion of the common interests of the citizens of the Union, of the European principles and values. In the vision of the High Representative of the European Union for Foreign Affairs and Security Policy, in this period marked by intense and especially continuous challenges, a strong Union must think strategically, share a common vision and, above all, act jointly.*

The European Union must continue to play a major role as a global security provider, as well. This is the objective of the new European Union Global Strategy for foreign policy and security.

Keywords: *defence, crises, global, borders, instability, security.*

1. Security – the main EU strategic concern

"*We need a stronger Europe. Our citizens deserve this, the whole world is waiting for it.*"[1]

Through the new Global Strategy for Foreign Policy and Security, the European Union has sought to strengthen its existing partnerships, but in particular to deepen its transatlantic connection. At the same time, the new Strategy wanted to develop new connections with the big global players and to make efficient and lasting investments, both at local and regional levels in order to increase the cooperation between the regions.

"*Our interests and values go hand in hand. We are interested in promoting our values in the world. At the same time, our core values are an integral part of our interests. Peace and security, prosperity, democracy and a global order based on norms are the vital interests that underline our external action*"[2], stressed Federica Mogherini. The aim of the reformed global governance was to meet the new challenges of this century. The new Global Strategy for foreign policy and security relies on practical and principled collaboration in which all responsibilities are shared, and the contribution comes from all members of the Union. It has always been considered that the weaknesses of our neighbours and partners are own weaknesses.

[1] Secretariatul General al Consiliului Uniunii Europene, *O strategie globală pentru politica externă și de securitate a Uniunii Europene* – format pdf, p.5.

[2] Secretariatul General al Consiliului Uniunii Europene, *O strategie globală pentru politica externă și de securitate a Uniunii Europene* – format pdf, p.11.

"*In developing of the new European Union Global Strategy for foreign policy and security, it was considered that all needs for change should be analysed and subsequently promoted through a unitary action and based on a system focused on multilateralism. The new European Union Global Strategy for the foreign policy and security has been elaborated specifically to manage global, regional, but also internal dynamics, to meet any new challenges of the superpowers, as well as to deal with increasing situations more unexpected*".[3]

In addition, the common bilateral security and defence policy brings new elements for the Eastern partners, new components in continuous intensification.[4]

The new European Union Global Strategy for the foreign and security policy (EUGS)[5] has been taken into discussion and supported in front of the European Council by Federica Mogherini, the High Representative of the European Union for Foreign Affairs and Security Policy and Vice-President of the European Commission, in June 28, 2016. The EUSR's motif is undoubtedly the security, but the focus is mainly on the strategic dialogue, just because of the EU's ability to strengthen cooperation between states on security and to reduce the uncertainty of the European and global security environment. There is an obvious paradigm change in relation to the European Security Strategy from 2003. The Strategic autonomy has been the motto of the EUGS of 2016.

2. Brief presentation of the European Union CSDP evolution

The previous Strategy of the European Union dated from 2003 and had been adopted during the mandate of the High Representative of the European Union for the Common Foreign and Security Policy, Javier Solana. That year, for the first time, the EU had agreed on a joint threat assessment and set goals to promote its security interests, based on core values. Javier Solana stated: "*A secure Europe in a better world is the ultimate goal of our actions*".[6]

The dialogue regarding the development and especially the modalities of putting the new Global Security Strategy into practice has been very intense and has taken place in several areas, since the preparation of the official launch of the document. This dialogue is ongoing at the level of the European institutions and all the Member States of the European Union.

"*The European Union was seen as a force for good in the international system. However, due to systemic changes in the international environment and crises of European integration, its role in the world has become somewhat controversial. Using the case of the EU Global Strategy (EUGS), this calls into question the effects of the emerging politicization for the political integration of the European Union*".[7]

Prior to the presentation of the new European Union Global Strategy for the foreign and security policy, the process of all aspects analysing and presenting the proposals has included also the organization of informing conferences of the EU Member States, within which the main topics addressed were relevant from the Strategy perspective. These events provided the opportunity that, alongside the governments of the Member States, to be able to express their positions the representatives of the academic environment and of the different institutional research institutes or other specialized organizations, in the context in which the process of developing a new Strategy was intended to be vast and inclusive.

[3] https://www.mae.ro/node/39086, accessed 09.03.2020.

[4] *European Union High Representative for Foreign Affairs and Security Policy*, Journal of European Studies, vol. 31, No 2, Decembrie 2005.

[5] https://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_ro_version.pdf accessed 10.03.2020.

[6] https://www.consilium.europa.eu/media/30815/qc7809568roc.pdf accessed 10.03.2020.

[7] https://www.tandfonline.com/doi/full/ accessed 11.03.2020.

Based on these considerations, the structure of the new European Union Global Strategy for foreign policy and security was elaborated, being focused on five major priorities: security of the European Union; the resilience of states and societies from the East and South of the Union; an integrated approach of the conflicts; regional orders based on cooperation; Global governance for the 21st century.

Since September 2016, under the coordination of the High Representative/Vice-President of the European Commission, Federica Mogherini, the European External Action Service, the EU member states have begun to work closely for the implementation of the Global Strategy in all areas of applicability.

Security of the European Union: The Union "*allows citizens to enjoy unprecedented security, democracy and prosperity. However, terrorism, hybrid threats, economic volatility, climate change and energy insecurity endanger the citizens and the territory of the European Union*".[8] An adequate level of strategic aspiration and autonomy is important for Europe in promoting peace and security inside and outside its borders. Therefore, the new Strategy will strengthen efforts on defence, cyber security, combating terrorism, energy and strategic communications. "*The Member States of the European Union must implement in practice their commitments on mutual assistance and solidarity, enshrined in the Treaties. The EU will step up its contribution to Europe's collective security, in close cooperation with its partners, starting with NATO*".[9]

Politics reconfigures the current geopolitical situation, being exceeded the moment of a Europe that cannot act synchronously.[10]

The resilience of states and society to the eastern and southern neighbourhoods: "*It is in the interest of the European Union's citizens to invest in the resilience of the states and societies that extend East to Central Asia and South to Central Africa. Within the European Neighbourhood Policy, many people want to establish closer relations with the Union: the power of the Union of attraction can stimulate transformation. Resilience is also a priority in other countries within and outside the European Neighbourhood Policy (ENP). The EU will support different pathways to resilience, targeting the most acute cases of government, economic, societal and climate/energy fragility and will develop more effective migration policies for Europe and its partners*."[11]

An Integrated Conflict Approach: When violent conflicts erupt, our common vital interests are threatened. Through the new European Union Global Strategy for foreign policy and security, the EU has been practically committed and based on the principles within the peacebuilding process and will promote security through an integrated approach. Implementing the global approach to conflict and crisis through the consistent use of all EU policies is essential. But the meaning and scope of the global approach will be further expanded. "*The EU will act at all stages of the conflict cycle, promptly in the prevention phase, responsibly and decisively in crises, investing in stabilization and avoiding premature disengagement when a new crisis breaks out. The EU will act at different levels of governance: conflicts such as those in Syria and Libya have local, national, regional and global dimensions that need to be addressed appropriately. A lasting peace can only be achieved through comprehensive agreements anchored in broad, deep and lasting regional and international partnerships, which the EU will promote and support*."[12]

[8] Secretariatul General al Consiliului Uniunii Europene, *O strategie globală pentru politica externă și de securitate a Uniunii Europene* – format pdf, p. 7.

[9] *Ibidem*, p. 8.

[10] Havier Solana, *Global challenges for the European Union Common Foreign Security Policy*, Military Technology, Bonn, Vol. 26, ISS 12, Dec 2002, pp. 9-14.

[11] Secretariatul General al Consiliului Uniunii Europene, *O strategie globală pentru politica externă și de securitate a Uniunii Europene* – format pdf, p. 7.

[12] *Ibidem*.

Regional cooperation systems: "*In a world caught between global pressures and local opposing reactions, regional dynamics play a vital role. Voluntary formulas of regional governance give states and peoples the opportunity to better manage security concerns, to take advantage of the economic benefits offered by globalization, to give a broader form of expression to cultures and identities and to influence international affairs. This is a fundamental principle for the peace and self-development of the EU in the 21st century, which is why we will support regional cooperation systems worldwide. In different regions - in Europe; in the Mediterranean area, the Middle East and Africa; along the Atlantic, both North and South; in Asia; and in the Arctic region - the EU will be guided by specific objectives*".[13]

Global governance for the 21st century: The EU is committed to developing a global order based on international law, which guarantees human rights, sustainable development and sustainable access to global common goods. "*This commitment translates into the aspiration to transform rather than simply maintain the current system. The EU will strive for a strong United Nations, as a cornerstone of norm-based multilateral order, and develop coordinated responses worldwide with international and regional organizations, state and non-state actors*".[14]

3. CSDP central concepts

Along with the implementation of the new European Union Global Strategy, there have been notable achievements in the security and defence package, in all its dimensions, the state and societal resilience in the neighbourhood, the integrated approach to crises and external conflicts, regional co-operative orders, governance and multilateralism based on rules.

A coherence was desired in the process of implementing the new Security Strategy of the European Union, in the decision-making process and in the allocation of resources, in order to ensure the necessary means for the EU to play the role of global player.

In the field of security and defence, the most advanced in terms of implementation, a series of progress has been recorded in support of the objectives assumed by the Union on this level: strengthening the operational dimension of the EU's commitment by creating the Planning Capacity and Conducting the non-executive Missions of the Union (MPCC), launching and operationalizing a package of initiatives, including the European Defence Fund (EDF), the Annual Coordinated Defence Analysis (CARD) and the Permanent Structured Cooperation (PESCO); strengthening the civil dimension of the PSAC; the continuation of the actions for the implementation of the agreed measures for the development of the NATO-EU cooperation framework (notable progress has been made regarding military mobility, cyber security, hybrid field, strategic communication and joint exercises).

4. Final discussions

"*The new Global Strategy for the foreign policy and security of the European Union is supported by the vision and ambition to create a stronger Union, willing to commit itself and especially able to make a difference for all its citizens. Existing directions of action that do not work will need to be revised, developed and implemented in line with the priorities of this strategy. However, the new Global Strategy will require regular review, in consultation with the Council, the Commission and the European Parliament. Each year the current state of the*

[13] Secretariatul General al Consiliului Uniunii Europene, *O strategie globală pentru politica externă și de securitate a Uniunii Europene* – format pdf, p. 8.
[14] *Ibidem.*

strategy will be analyzed and updates, repositions and adjustments will be made permanently so that it is further implemented".[15]

"*As regards the priorities identified by the new Global Strategy of the European Union, the High Representative, supported by Member States with similar ideas, could gradually introduce a more flexible decision-making practice. In other words, to keep the strategy relevant, it must be limited in time. No action agenda can remain relevant for more than one mandate. Therefore, it is better to provide in the Global Security Strategy of the European Union that it will be reviewed within five years of its adoption. If we can learn from the missed opportunities from the past, there is no reason not to get the process right this time.*"

Also, a new strategic reflection process will be launched whenever the European Union and its Member States deem it necessary to enable the Union to make effective progress. Our citizens deserve a true Union, which promotes our common interests by engaging responsibly and establishing partnerships with others.

Romania has been consistently involved in the process of conceptual development of the Strategy, and subsequently, in the implementation process. The national contributions were built on the basis of interests, as well as the significant expertise held, mainly related to the Black Sea region and the Eastern Neighbourhood.

Previously, but also during the presidency of the Council of the European Union, Romania encouraged the continuation of the implementation of the new Global Strategy for the European Union's foreign and security policy, especially in the fields of security and defence, resilience, stabilization and integrated approach in conflict and crisis management, regional cooperation in the Black Sea region, concomitant with the commitments towards strengthening the role of the European Union in a rules-based multilateral international order.

BIBLIOGRAPHY

1. Sven Biscop, *EU Global Strategy Expert Opinion*, EU Institute for Security Studies, 2016;
2. The General Secretariat of the Council, *A Global Strategy for the Foreign and Security Policy of the European Union* - June 28, 2016, pdf format;
3. *European Union High Representative for Foreign Affairs and Security Policy*, Journal of European Studies, Vol. 31, No 2, Decembrie 2005;
4. Havier Solana, *Global challenges for the European Union Common Foreign Security Policy*, Military Technology, Bonn, Vol. 26, ISS 12, Dec 2002;
5. https://www.mae.ro/node/39086
6. https://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_ro_format.pdf
7. https://www.consilium.europa.eu/media/30815/qc7809568roc. pdf format
8. https://www.tandfonline.com/doi/full/

[15] Secretariatul General al Consiliului Uniunii Europene, *O strategie globală pentru politica externă și de securitate a Uniunii Europene* – format pdf, p. 45.

NATO and EU Policies and Strategies

Chairs:

Cosmin Florian OLARIU, PhD
Cristian ICHIMESCU, PhD

THE EU FUNDS – THE NEW STRATEGIC MECHANISM FOR ENFORCING THE RULE OF LAW DIMENSION IN THE PROGRAMING PERIOD 2021-2027

Lăcrămioara Gena PARASCHIV
Ph.D Student, Doctoral School for Public Order and National Security,
Police Academy "Alexandru Ioan Cuza" of Bucharest, Romania,
lacramioaragena@yahoo.com

Abstract: *Lately the EU legal order faced a rule of law crisis that impacted both Member States judicial systems and EU finances area. In this respect, EU challenged itself to "enforce" rule of law at national level. Considering that this enforcing process couldn't be done directly but in a complementary way combining political dialogue with legislative tools and judicial norm application, one may consider that the Union found the solution in linking the sound management of EU spending to the rule of law. In the light of the programming period 2021-2027 the respect for the rule of law at national level became "a prerequisite" that the EU finances are "sufficiently" safeguarded.*

Keywords: *funds, rule of law, sound management.*

Introduction. The concept of the rule of law promoted by the EU legal order

As recognized by the European Court of Justice, the European Court of Human Rights and European Commission (EC) the rule of law is a multidisciplinary concept that involves ensuring and delivering transparent and accountable "*legal protection"*[1] in all the areas covered by the European laws, effective, impartial and independent justice system, "*robust anti-corruption frameworks"*[2], separation of powers, impeding discretionary exercise of executive power and also ensuring respect for fundamental freedoms and rights and equality under the law.

As one can see, for the European Union (EU) the rule of law concept is a methodological and embracing one that creates an environment indispensable for the achievement of the EU' objectives as regards strengthening good governance in the Union's justice and security area.

Following this approach, the rule of law is imposed as a fundamental value for the EU as reflected in the Treaty on European Union (TEU) and the Charter of the Fundamental Rights of the European Union[3] (CFR). Thereby, in the Preamble and Article 2 of the TEU, the Member States recognize that the rule of law is a *"value",* a *"common"* value. Furthermore, in the Preamble and provisions of Article 41 and Article 47 of the CFR the Member States engage to contribute to *"the development of [...] common values"* guaranteeing, among other rights, *"the right to a good administration"* and *"the right to an effective remedy and to a fair trial".*

[1] *Consolidated version of the Treaty on European Union*, OJ C no. 202 from 7 June 2016, pp. 13-47, Art. 19, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2016:202:TOC, accessed 10 of February 2020.

[2] European Commission, Communication from the Commission to the European Parliament, the European Council and the Council, *Further strengthening the Rule of Law within the Union, State of play and possible next steps*, Brussels, 3.4.2019 COM(2019) 163 final, p. 2, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0163&from=EN accessed February 10, 2020.

[3] *Charter of the Fundamental Rights of the European Union*, OJ C no.202 from 7 June 2016, pp.389-404, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2016:202:TOC accessed February 10, 2020.

In the recent Communication *Further strengthening the Rule of Law within the Union*[4], EC revives this broad conceptualization of the rule of law. The Commission states that the rule of law is of quintessential relevance for the future of the Union and, in this respect, all the public authorities must act and *"every action taken by the EU"*[5] must be executed under the legal constraints and under the control of an independent and impartial judicial system.

The last confirmation of this embracing conceptualization is confirmed by the EC in the Communication, *Strengthening the rule of law within the Union. A blueprint for action* of July 2019[6] which states that the rule of law is *"well-defined in its core meaning"*[7] by the European primary and secondary law and that the Member States, taking into account the principle of EU law primacy and the principle of sincere cooperation, despite their different legal systems, are bound to safeguard and respect.

Therefore, in both communications, EC highlights that, although the value of the rule of law is fundamental ethical, it deserves enforceable meaning and also requires transpositions into judicial regulations. This approach is justified by the fact that the respect of the rule of law is a major obligation for Member States and any violation of this imperative worth having legal consequences.

Since the respect of the rule of law became the *"bedrock"*[8] of the Union's democratic functionality, EC committed itself to urgently address the enforcement of the rule of law using complementarily political and legal mechanisms.

EU mechanisms that protects the rule of law

As established in the above mentioned Communications of April 2019 and of July 2019, EU may apply political and legal mechanisms in order to address issues rose by the way Member States understand or not to protect the rule of law at the national level.

The political response may trigger *"the preventive and sanctioning"*[9] Art.7 of TEU and "*the EU Framework to strengthen the Rule of Law"*[10] and the legal response may take the form of infringement proceedings namely *"effective judicial protection"*[11] according to the provision of Article 258 of the Treaty on the Functioning of the European Union[12] (TFEU).

While the Art.7 of TEU and the Rule of Law Framework may be activated when the EU law aspect is affected respectively may be activated preventively when a *"clear risk of a*

[4] European Commission, Communication from the Commission to the European Parliament, the European Council and the Council, *Further strengthening the Rule of Law within the Union, State of play and possible next steps,* Brussels, 3.4.2019 COM(2019) 163 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri =CELEX:52019DC0163&from=EN accessed February 10, 2020.

[5] *Ibidem*, p. 1.

[6] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *Strengthening the rule of law within the Union A blueprint for action,* Brussels, 17.7.2019 COM(2019) 343 final, https://ec.europa.eu/info/sites/info/files/7_en_act_part1.pdf, accessed February 10, 2020.

[7] *Ibidem,* p.1.

[8] *Ibidem.*

[9] European Commission, Communication from the Commission to the European Parliament and the Council, *A new EU Framework to strengthen the Rule of Law,* Strasbourg, 11.3.2014 COM(2014) 158 final, p.5, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0158&from=RO, accessed February 12, 2020

[10] *Ibidem,* p. 6.

[11] European Commission, Communication from the Commission to the European Parliament, the European Council and the Council, *Further strengthening the Rule of Law within the Union, State of play and possible next steps,* Brussels, 3.4.2019 COM(2019) 163 final, p. 4 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/? uri=CELEX:52019DC0163&from=EN, accessed February 12, 2020.

[12] *Consolidated version of the Treaty on the Functioning of the European Union*, OJ C no.202 from 7 June 2016, pp.47-200, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12016E/TXT&from=EN, accessed February 12, 2020.

serious breach"[13] (At.7 paragraph (1)) is identified or sanctionably when Member States persists in serious breaches of law (At.7 paragraph (2)) or when Member States apply measures that compromise *"systematically and adversely"*[14] the functionality of national public institutions that are responsible in safeguarding the rule of law, the legal mechanism of infringement proceedings is activated to tackle any breach in fulfilling any obligation stipulated in the Treaties.

But with the Communications of April 2019 and of July 2019, EU clearly set out a new practical approach establishing and, as we can see, completing the legal and political mechanisms, another category of *"warning and preventive"*[15] mechanisms for protecting the rule of law. This category includes The European Semester, The annual EU Justice Scoreboard, The Cooperation and Verification Mechanism, The Commission's Structural Reform Support Service, The European Structural and Investment Funds, A new mechanism to protect the Union's budget when generalised deficiencies regarding the rule of law in Member States affect or risk affecting that budget[16], The European Anti-Fraud Office (OLAF), the European Public Prosecutor's Office (EPPO) and Annual Rule of Law Report.

As one can observe analysing this category which we may entitle *"strategic mechanisms"*, half of them are teleologically oriented to the protection of the European financial interests. This hypothesis leads us to the conclusion that the EC approaches the protection of the EU funds from a rule of law angle.

Conversely, if EC creates this linkage between the respect of the rule of law and the implementation of a sound financial management of EU funds and budget we may deduce that for the EC, in the programming period 2021-2027, the European financial interests will play a crucial role in supporting the *"enforcement"* of the rule of law dimension.

Why the EU funds are the new strategic mechanism for *"enforcing"* the Union's rule of law dimension

The enforcement feature of the rule of law dimension in the Commission's proposed regulations and communications clearly emphasizes the role of EU funds.

With the *Communication A new, modern Multiannual Financial Framework for a European Union that delivers efficiently on its priorities post-2020*[17] of February 2018 EC opened the way to new operational enforcements as regard the rule of law setting that the Financial Framework 2021-2027 is the right moment to reflect on how the connection between EU funds and the respect for the Union's key values *"can be strengthened"*[18].

Furthermore, in the *Proposal for a Regulation of the European Parliament and of the Council on the protection of the Union's budget in case of generalised deficiencies as regards the rule of law in the Member States* of May 2018, EC pointed out the fact that the potential of

[13] European Commission, Communication from the Commission to the European Parliament, the European Council and the Council, *Further strengthening the Rule of Law within the Union, State of play and possible next steps,* Brussels, 3.4.2019 COM(2019) 163 final, p. 5, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0163&from=EN accessed February 12, 2020.

[14] *Ibidem*, p. 6.

[15] *Ibidem*, p. 4.

[16] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of the Union's budget in case of generalised deficiencies as regards the rule of law in the Member States,* Brussels, 2.5.2018 COM(2018) 324 final, https://ec.europa.eu/commission/sites/beta-political/files/protection-union-budget-rule-law-may2018_en.pdf accessed February 12, 2020.

[17] European Commission, Communication from the Commission to the European Parliament, the European Council and the Council, *A new, modern Multiannual Financial Framework for a European Union that delivers efficiently on its priorities post-2020,* Brussels, 14.2.2018 COM(2018) 98 final, https://ec.europa.eu/ commission/sites/beta-political/files/communication-new-modern-multiannual-financial-framework_en.pdf accessed February 15, 2020.

[18] *Ibidem*, p. 16.

the Union's budget can be achieved only if the Member States' administrative environment and institutional capacities is beneficial. A sound financial management of EU funding can't be effective unless seconded by a fruitful application of legal and administrative measures that secure the respect of the rule of law. With this proposal EC introduced the respect for the rule of law as a *"prerequisite for confidence"*[19] that the EU spending are adequately safeguarded.

But the main added value of the *"enforcement"* of the rule of law dimension is expressed in the Communications of April 2019 and of July 2019 that connect the respect of the rule of law with fighting fraud and corruption that impact the EU spending. Within these two communications the Commission enunciates a more proactive and practical approach as regards ensuring the respect of rule of law in Member States in the Multiannual Financial Framework (MFF) 2021-2027 using a set of operational mechanisms that are intrinsically linked to the fulfilment of its responsibility as a guardian of the EU budget.

The Communications make direct references, first of all, to the European Semester evaluations as they were proposed to be introduced in the Common Provision Regulation for the future MFF 2021-2027[20]. EC states that, taking into consideration that the European Semester (ES) annual evaluation is a *"key to boosting investment"*[21] in all socio-economic areas including the legal and judicial area, it is necessary that the ES country reports be used as a practical tool for evaluating and guiding Member States sectoral investment necessities and *"programming decisions"*[22] for the Cohesion Policy during MFF 2021-2027 and, most of all, for assessing the robustness of the rule of law dimension namely the anti-fraud environment created by the national public authorities including those responsible for EU spending management.

Secondly, the Communications make reference to the process of absorption of EU structural and investment funds, a process that becomes fundamental for the consolidation of Member States institutional capacity to fight fraud and corruption. Using the mechanism of *Commission Anti-Fraud Strategy*[23] (CAFS), EC expects to be very active in protecting the EU funds. In this connection, in order to ensure a sound financial management in the MMF 2012-20127, the Commission concentrates its efforts towards diminishing and removing the vulnerabilities of the internal control systems and formulates its commitment to further improve data collections regarding the fraud and corruption patters and the profiles of the fraudsters namely to develop the Early Detection and Exclusion System and the Irregularity Management System. Plus EC engages itself in optimizing *"coordination, cooperation and*

[19] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of the Union's budget in case of generalised deficiencies as regards the rule of law in the Member States*, Brussels, 2.5.2018 COM(2018) 324 final, p. 1, https://ec.europa.eu/commission/sites/beta-political/files/protection-union-budget-rule-law-may2018_en.pdf accessed February 13, 2020.

[20] European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down common provisions on the European Regional Development Fund, the European Social Fund Plus, the Cohesion Fund, and the European Maritime and Fisheries Fund and financial rules for those and for the Asylum and Migration Fund, the Internal Security Fund and the Border Management and Visa Instrument*, Strasbourg, 29.5.2018 COM(2018) 375 final, https://eur-lex.europa.eu/resource.html?uri=cellar:26b02a36-6376-11e8-ab9c-01aa75ed71a1.0003.02/DOC_1&format=PDF accessed February 15, 2020.

[21] European Commission, Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank, *Annual Growth Survey 2019: For a stronger Europe in the face of global uncertainty,* Brussels, 21.11.2018 COM(2018) 770 final, p. 10, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0770&from=RO accessed February 15, 2020.

[22] *Ibidem*.

[23] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the Court of Auditors, *Commission Anti-Fraud Strategy: enhanced action to protect the EU budge*t, Brussels, 29.4.2019, COM (2019) 196 final, https://ec.europa.eu/anti-fraud/sites/antifraud/files/2019_commission_anti_fraud_strategy_en.pdf accessed February 15, 2020.

workflows"[24] in the anti-fraud and anti-corruption fight with all the Commission agencies and services that are responsible to implement, in this respect, at every service level, sectoral anti-fraud strategies or joint anti-fraud strategies.

Thirdly, in the light of this objective of optimizing the cooperation between the Commission agencies, in the Communication of April 2019, EC expresses its commitment to strengthen the EU anti-fraud and anti-corruption institutional framework for Union financial security. One again the essential added value of the *"enforcement"* of the rule of law dimension in highlighted. EC advocates for the fruitful cooperation between the two institutional mechanisms namely OLAF, with its detection and investigative role of in fighting against fraud and corruption that affects the European financial interests, and EPPO, with its qualitative improvement that brings, once it become operational at the end of 2020, in the process of investigating, prosecuting and bringing to judgement the crimes against Union budget.

Fourthly, EC still keeps on its political agenda and remains firm in introducing and using the sanctionary mechanism of suspension and reduction of funding as suggested in *Proposal for a Regulation of the European Parliament and of the Council on the protection of the Union's budget in case of generalised deficiencies as regards the rule of law in the Member States* of May 2019 in the future financial regulations as regard the implementation of MFF 2021-2027.

Not at least, EC engages itself to monitor the functionality of all these mechanisms using a consolidated mechanism namely the Rule of law report, as proposed in the Communication of July 2019. Using this report as a redressing mechanism, EC wants to permanently have access to the *"significant developments"*[25] of rule of law in the Member States both in terms of good practices in the implementation of *"rule of law standards"*[26] and in terms of *"recurrent problems"*[27]. Taking into consideration that the report will comprise data from the ES annual country reports we may assume that this mechanism addresses also the problems related to the anti-fraud and anti-corruption measures implemented by the national public authorities responsible with the EU spending financial management.

Conclusions

One of the most important contributions of the Communications of April 2019 and of July 2019 was this new approach of the protection of the EU funds from a rule of law angle. But what is innovative in this respect is the way EC concentrates its efforts to change not only the level of action, that seems to be relocated from the national level to the supranational level, but the nature of action from using enhancing mechanisms to using "*enforcing*" mechanisms.

This enforcement aspect of the rule of law dimension in the process of ensuring the protection of the EU funds is emphasized by the way in which EC strategically organized the operational mechanisms to complement and mutually reinforce one another. We have the European Semester country reports and CAFS as preventive mechanisms, OLAF and EPPO as criminal sanctions mechanisms, the suspension and reduction of funding mechanism and, not at least, The Annual Rule of law report as a redress mechanism.

[24] *Ibidem*, p. 16.

[25] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *Strengthening the rule of law within the Union A blueprint for action*, Brussels, 17.7.2019 COM(2019) 343 final, p.11 https://ec.europa.eu/info/sites/info/files/7_en_act_part1.pdf accessed February 15, 2020.

[26] *Ibidem*.

[27] *Ibidem*.

Besides the clear will of Member states to soundly manage the EU spending, all of these mechanisms will unquestionably contribute to the enforcement of the rule of law dimension in MFF 2021-2027.

BIBLIOGRAPHY

1. European Commission, Communication from the Commission to the European Parliament, the European Council and the Council, *A new, modern Multiannual Financial Framework for a European Union that delivers efficiently on its priorities post-2020,* Brussels, 14.2.2018 COM(2018) 98 final.
2. European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of the Union's budget in case of generalised deficiencies as regards the rule of law in the Member States*, Brussels, 2.5.2018 COM(2018) 324 final.
3. European Commission, Communication from the Commission to the European Parliament, the European Council and the Council, *Further strengthening the Rule of Law within the Union, State of play and possible next steps,* Brussels, 3.4.2019 COM(2019) 163 final.
4. European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the Court of Auditors, *Commission Anti-Fraud Strategy: enhanced action to protect the EU budge*t, Brussels, 29.4.2019, COM(2019) 196 final.
5. European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *Strengthening the rule of law within the Union A blueprint for action,* Brussels, 17.7.2019 COM(2019) 343 final.

ROMANIAN EXTERNAL CHALLENGES WITHIN THE 2020 SECURITY ENVIRONMENT

Emil ȘERBAN
"Carol I" National Defence University,
emilserban.ro@gmail.com

Cristian ICHIMESCU, PhD
"Carol I" National Defence University,
cristian.ichimescu@yahoo.com

Abstract: *The 2020 security environment is characterized by complexity, volatility and unpredictability, with on-going military threats but other multiple domains that have to be addressed, taking into account their interconnectivity. Despite the Russian military security threat, Romania has to address imminent priorities like Brexit and the COVID 19 epidemic, generating the need for a comprehensive approach on defence and security. The paper will address the necessity of developing the national defence strategy into a more comprehensive national security strategy, suitable to address all the security domains in accordance with the complex security environment. Romanian subject matter experts have to think of migrating from a national defence strategy into a national security strategy, projecting Romania's interest in the long term, with legal possibilities to update it due to major shifts within the environment, rather than internal elections. Due to all challenges within the 2020 defence environment, Romania's political and military leaders have to update the threats already perceived in 2015, address the newly emerged ones and take positive measures in order to limit the country's vulnerabilities, while increasing its capacity to respond. The article contains two analysing tables on the threats based on risks and effects. All the threats represent key aspects that have to be included in future Romanian security strategies. In order to try to determine their priority for the Romanian authorities, the analysing tables will compare threats based on six criteria, with different ratios, context, probability, effects in the long term, vulnerability to the threat, capability to counter, and the potential support from the allies in NATO and EU. The final score of every threat will determine if the menace is of imminent priority, high priority, medium priority or low priority.*

Keywords: *aggressions, challenges, defence, strategy, threats.*

Following the severe psychological wounds of World War II, European societies established multiple mechanisms to avoid repeating such large-scale conflicts, with NATO and the EU as pillars of security and stability. Throughout the last seven decades, Europe avoided military conflicts, with some exceptions within the Balkans and the former USSR, setting up the conditions to believe that the development of diplomacy, economic prosperity and the human superior tolerance resulted in the decrease of the military threats against most of the European states.

However, in the 2020 complex and volatile security environment, Europe must face diverse challenges, not excluding military aggressions, particularly after the development of the on-going conflicts in Ukraine, but also taking into account the variety of threats emerging from non-military security domains, such as economic, political, societal and environmental[1].

Introduction

For the last 15 years, Romania has successfully maintained its western integration path, achieving full integration within the North Atlantic Treaty Organisation (NATO) and the European Union (EU), which added guarantees to the national security. According to the National Defence Strategy, "*the main warranty provider when it comes to Romania's security*

[1] The security domains according to the Copenhagen School.

is NATO", depending on the USA to maintain its commitment in Europe and the organisation's solidity. The most recent strategy from 2015 "*highlights the Russian Federation's activity in the Black Sea Region*", the emerging terrorism and "*Islamic radicalization phenomenon on European level*", and the intensification of poor economic migration from conflict areas and associated challenges to manage the flow[2].

At the regional level, Romania planned to maintain the strategic balance at the crossroad of regional security complexes and to contribute to the strengthening of the Europeanization process by a gradual extension of the European standards. On the contrary, the Russian Federation was assessed as trying to consolidate its status as a regional power, its actions having an impact on the European path of Ukraine, the Republic of Moldova and Georgia[3]. Very similar to the national security or defence strategies of Bulgaria, Poland and the Baltic Republics[4] within the same time framework[5] and updated with cyber security strategies, the Romanian Defence Strategy 2015-2019 underlines the threats posed by "*the actions performed to destabilize the eastern vicinity, the perpetuation of frozen conflicts in the Black Sea Region, the instability in the western Balkans, cyber threats, terrorism, the proliferation of the weapons of mass-destruction, and hostile intelligence actions*"[6].

In 2020 Romania remains on NATO and EU's eastern frontiers, in the vicinity of Russian military aggression and frozen conflicts within the Black Sea Region. Moreover, as part of a weakened European community after Brexit, corroborated with the potential for pan-European populism and extremism, terrorist menaces, the potential for mass migration and additional regional and global societal and economic challenges, Romania has to handle a multitude of external threats in all security-related domains. The current paper will analyse the relevance of the previously assessed threats and the newly emerged ones, corroborated with the associated vulnerabilities, trying to assess the Romanian priorities to counter the external security challenges after 2020. Furthermore, the paper will address the necessity of developing the national defence strategy into a more comprehensive national security strategy, suitable to address all the security domains in accordance with the complex security environment. The article will consist of two interesting approaches *The level of military threats to national security* and *The complexity of the non-military threats in 2020* and in the end *In place of conclusions: External threats assessment – Romanian priorities.*

1. The level of military threats to national security

In order to characterize the level of military threats to national security we have to assess the current relevance of war and military security, to explain the main forms of military aggressions in 2020 and to understand the current military security concerns for Romania.

The current relevance of war and military security

After the end of the First World War, multiple peace initiatives evolved in order to limit the prospective for a repeating massive armed confrontation. The Second World War's

[2] The Presidential Administration, *National Defence Strategy 2015-2019 – A Strong Romania within Europe and the World*, Bucharest, 2015, pp. 11-13.

[3] *Ibidem*, p. 13.

[4] In NATO's common terminology the Baltic Republics or the Baltic States include Lithuania, Latvia and Estonia.

[5] Bulgarian National Assembly, *National Security Strategy of the Republic of Bulgaria*, 2011; Estonian Ministry of Defence, *National Defence Strategy Estonia*, 2011; Seimas of the Republic of *Lithuania, The National Security Strategy*, Resolution No XIII-202, 2017; The Republic of Latvia, *The National Security Concept* (informative section) https://www.mod.gov.lv/sites/mod/files/document/NDK_ENG_final.pdf; The President of Poland, *The National Security Strategy of The Republic of Poland*, 2014.

[6] The Presidential Administration, *National Defence Strategy 2015-2019 – A Strong Romania within Europe and the World*, Bucharest, 2015, pp. 14-15.

experience consolidated the need for peace, therefore international institutions, particularly the United Nations (UN), accelerated the process towards a more peaceful world. The UN succeeded multiple times to discourage, limit or avoid mass military confrontation, and despite any partial failures, appears to question the relevance of war as a tool in modern foreign policy. However, the war, in its conventional form, did not disappear as a practice, but rather develops within a UN peace promoted environment, usually against the weakest. The war of the smaller state entities is usually arbitrated by the major actors, while global powers can easily veto any involvement in their or their allies' conflicts. The UN appears as a subjective system, as it allows the Security Council's permanent member to dictate the consistency of international involvement in wars, and to block any intervention in conflicts supporting their interests[7], with a current example in the already eight-year-long Syrian conflict.

The development of diplomacy does not reflect on the state actors' appetite for defence budgets. The numbers are particularly curious as the top countries by annual military expenditure were just marginally affected by foreign aggressors in the last seven decades, USA, China, Saudi Arabia, Russia, India, France, United Kingdom, Japan, Germany, South Korea, Brazil, Italy, Australia, Canada, and Turkey, which share approximately 80% of the global defence spending[8]. The perception of strength appears to remain unchanged in modern inter-state relations, with super-powers' intimidation strategy through their military capabilities and sometimes even aggressions in support of their interests.

The present society is at the historic lowest risk of dying in armed conflicts which may build the perception of foreseeable peace, but even in Europe, war is an on-going phenomenon after 2014. Despite the codification of *jus contra bellum* as a primary rule governing the conduct of international relations, military strength and war remain valuable instruments to the detriment of weaker states, which either do not have the necessary capability to wage war or prefer other means to settle their international disputes[9].

Forms of military aggressions in 2020

Modern conflicts highlight the complexity of the operational environment, with state and non-state actors, an additional cyber environment, and multiple additional targets to the conventional military installation. Post World Wars conflicts were characterized by the usage of proxy elements, while contemporary aggressions added hybrid tactics and cyber-attacks, all increasing states' deniability and preserving the perception of peace among super-powers.

The practice of using proxy elements in conflicts is not necessarily new, but their scale increased exponentially during the Cold War. Moreover, due to the need of officially promoting peace while also protecting other national interests, proxy conflicts developed in the 21st century, with on-going examples in Afghanistan, Iraq, Syria, Yemen, Libya, Ukraine etc.

The hybrid warfare's characteristics became obvious particularly throughout Russian aggression in Crimea and Eastern Ukraine[10]. Propaganda, deception, sabotage and other military and non-military tactics have long been used to destabilise the enemy, but in the last decades, they increased in speed, scale and intensity, facilitated by rapid technological change

[7] United Nations, *Charter of the United Nations and Statute of the International Court of Justice*, Chapter V, San Francisco, 1945.

[8] Emma Beswick, *Which countries spend the most on their military?*, EuroNews, 2018 https://www.euronews.com/2018/05/02/which-country-spent-the-most-on-its-military-in-2017- accessed Feb. 15, 2020.

[9] Vilém Kolín, *The Role of War in International Politics*, Úloha Války V Mezinárodní Politice, https://www.obranaastrategie.cz/filemanager/files/6265-en.pdf accessed Feb. 15, 2020.

[10] *NATO's response to hybrid threats*, Last updated: 08 Aug. 2019, https://www.nato.int/cps/en/natohq/topics_156338.htm, accessed Feb. 16, 2020.

and global interconnectivity, setting up the framework for high-efficiency hybrid operations[11].

Cyber aggressions are usually part of complex hybrid conflicts, but are also used as independent forms of conflict bringing unique implications in communication and transport systems or water and electricity supplies[12]. They represent one of the only direct aggressions between major powers and security organizations of the world due to the supreme level of deniability. Moreover, cyber operations affect the vast majority of the society, not only military installations, often putting significant pressure on political leaders, which have to respond as fast as possible to the incidents. Also, cyber aggressions are associated with a larger pool of combatants, from state entities to non-state actors, such as economic competitors or terrorist organizations, which exploit the commercial of the shelf technologies for cyber-attacks.

Overall, the modern warfare combines military with non-military procedures, the show of force with efficient propaganda and strategic communication, and the physical battle space with the virtual environment, sometimes reducing the gap between asymmetric opponents and increasing the difficulty to accurately assess the threat.

Current military security concerns for Romania

Even though the end of the Cold War corroborated with the process of integration into NATO should put Romania at a lower military security risk, the reality of 2020 appears to be different. However, within the 2020 operational environment, with less than 200 miles from the Russian fleet in Sevastopol and the Russian annexed Crimea, a conventional military aggression against a NATO member, including Romania, does not look as doubtful as 10 years ago. The complexity of the modern warfare enables hybrid, cyber and terrorist operations, particularly due to the country's geostrategic position on the Euro-Atlantic block's border. Besides, military aggression against other countries and other events within the political or socio-economic domains could affect Romania's military security.

From the conventional aggression perspective, the last decade's main events shaped the current operational environment. The western diplomatic effort to integrate former Soviet Union republics after the successful examples of the Baltic States was probably perceived as a NATO/EU attempt to "*conquer*" Russia's historic areas of influence. The possibility of Ukraine and Georgia's Euro-Atlantic integration triggered a spike in Russian military expenditure, which in 2013 adopted a multi-year plan with major increases in defence spending budgeted each year until 2020[13]. Russia started to allocate a higher percentage of GDP for defence, overpassed the average 4% allocated by the USA[14], which created the conditions for the proxy and direct aggression in Ukraine and the "*show of force*" in Syria.

Regardless of the measures taken by the western allies, to grow NATO's military expenditures, particularly in Eastern Europe[15], with Romania one of the first countries to spend 2% of the GDP for defence[16], the conventional military aggression cannot be ruled out.

[11] Bret Perry, *Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations*, Small War's Journal, https://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera, accessed Feb. 18, 2020.

[12] University of Cambridge, Cambridge Dictionary, 2018, Cyber warfare definition, https://dictionary.cambridge.org/dictionary/english/cyber-warfare, accessed Feb. 18, 2020.

[13] Nikolas K. Gvosdev, The Bear Awakens: Russia's Military Is Back, The National Interest, November 12, 2014, https://nationalinterest.org/commentary/russias-military-back-9181, accessed Feb. 18, 2020.

[14] Max Roser, Mohamed Nagdy, *Military Spending, Empirical View*, Our world Data, https://ourworldindata.org/military-spending, accessed Feb. 20, 2020.

[15] Fenella McGerty, Jane's Defence Budgets - Global Budgets Trends, Jane's Defence, 13 March 2018, https://www.janes.com/article/78514/jane-s-defence-budgets-global-budgets-trends-2018, accessed Feb. 20, 2020.

[16] *Pactul pentru Apărare a fost semnat. Președintele: Este un acord implicit pentru dezvoltarea industriei naționale de apărare*, 13.01.2015, https://www.digi24.ro/stiri/actualitate/politica/pactul-pentru-aparare-a-fost-

The main military likely threat comes from Russia, which maintains troops in Transnistria and deployed substantial military installations within the Black Sea region. However, despite a major shift in NATO's integrity, the direct aggression against Romania from the East is assessed with a low probability. Moreover, potential military aggression from other state entity is almost certainly hard to project. For the moment all the neighbours are allies or have no obvious intention to start any military action against Romania.

Taking into account a hybrid aggression against Romania, the country presents some vulnerability to external propaganda targeting dissident ethnic and social groups. Romanian population is under continuous propaganda against NATO, which should create the basis for possible local support in case of hybrid aggression. However, the Romanian population is largely western oriented, and generally nationalistic homogenous, therefore, in the context of no major changes in the Euro-Atlantic unity, a hybrid conflict on Romanian soil is unlikely in the short-to-midterm. However, due to the position in the vicinity of Russia and its proxy elements from Ukraine and Moldova, Serbia as main Euro-Asian ally in the Balkans, and Hungary with an inconsistent position within the European community, the development of possible hybrid threats in the long term has to be seriously analysed and countered.

The cyber threat is probably the most credible aggression in the short-to-midterm. As a member of NATO and the European community, with NATO and US military installations on the ground, Romania is probably a target of the European and American contenders. Romanian networks could face cyber-attacks especially due to their secondary effects on NATO and EU's interests or as a show of force and intimidation strategy for the entire Euro-Atlantic society. From this perspective, the pool of potential aggressors resides much further than Romania's geographical vicinity, countries known to target NATO and EU though cyber-attacks ranging from the Russian Federation and China, up to Iran, North Korea and others. Romania has taken preventive measures by adopting a specific strategy to counter cyber threats[17], integrate within the European Union Agency for Cybersecurity, and developing cybersecurity units, including the Romanian Intelligence Service's Cybersecurity Department[18], the National Computer Incidence Response Team[19], and the newly established Armed Forces Cybersecurity Command[20]. Therefore, despite the high probability threat, Romania and its partners are constantly addressing the likely menace being able to deal with most of possible cyber incidents. Also, as Romania has not reached a high level of digitalisation yet, comparable with its western allies, the impact of a major cyber aggression on the Romanian society is likely to remain limited. However, one must not neglect the fact that Romania has been actively involved in the Three Seas Initiative, whose third component is focused on accentuated digitalization. Within the Initiative, Romania would like to enhance its role as a regional security-provider, which is likely to step up its emphasis on digital policies[21], which will most likely become vulnerabilities for the country, and add up, in the medium and long-term to its agenda of threats, risks and vulnerabilities.

Terrorism has been a major threat for the European society within the last decade, particularly due to ISIS and its lone-wolf recruited fighters. Taking into account the recent defeat of the Caliphate in their heartland from Syria and Iraq, the probability of fighters to

semnat-presedintele-este-un-acord-implicit-pentru-dezvoltarea-industriei-nationale-de-aparare-346358, accessed Feb. 20, 2020.

[17] Romanian National Government, *Cyber Security Strategy of Romania*, 2013.

[18] https://www.sri.ro/cyberint

[19] https://cert.ro/

[20] https://www.cybercommand.ro/

[21] Oana-Elena Brânda, *The Three-Seas Initiative – A New Role for Romania?*, Proceedings of the International Conference ”Defence Resources Management in the 21st century”, Brașov, ”Carol I” National Defense University Publishing House, 2018, pp. 86-87, http://www.codrm.eu/conferences/2018/Carte%20CoDRM%202018.pdf, accessed Feb. 26, 2020.

return to their residence countries in Europe or from other ISIS adepts to come to Europe has increased significantly. On the other hand, Romania has not been an ISIS recruiting pool, with no Romanian citizen reported as a fighter in the Middle East or Europe. Furthermore, Romania’s Islamic community is traditionally peaceful, fully integrated, and opposing any forms of extremism, while among the mixed families with ties to the Middle East, fundamentalist and extremist views were marginally reported. Above all those, the national security services have proven high competence in fighting terrorism and extremism over the last 3 decades, the risk of major terrorist incidents on Romanian soil likely staying low. Still, Romania must address the threat seriously, to avoid further incidents or to stop the possible facilitation networks operations through its national territories in support of the terrorist groups in Western Europe.

Analysing other external conditions that could affect Romania’s defence strategy, an escalation of the fight in Ukraine or a resurgence of conflict in the Republic of Moldova are probably the most dangerous scenarios. In addition, there are other key political and economic shifts that may affect Romania’s military security in the long term, with examples like the American isolationist agenda, the volatile foreign policy of Turkey and Brexit.

A possible Russian intensification of the military activity in Eastern Ukraine, generating conventional conflict against the Ukrainian Armed Forces, is highly likely to have a negative impact on NATO in general. For Romania, a possible extension of the fighting area towards its border, especially corroborated with the Russian Forces already present in Transnistria, is extremely dangerous. Also, another possible Russian annexation of territories is another red line which will probably have a major impact on NATO’s cohesion and pose additional threats to Romania due to the almost certain Russian military strategic installations redeployment closer to Romanian borders. However, at least in the short-to-midterm, the conflict appears to have frozen, similarly to other Russian interventions in the USSR’s former territories. The Russian Federation apparently consolidates Crimea and has an interest in preserving the current instability and hybrid aggression in Eastern Ukraine, therefore the probability of escalation is assessed as low-to-medium.

The Republic of Moldova is under heavy Russian influence, which has proxy political elements and conducts an aggressive information operations campaign. The Russian Federation probably maintains capabilities to initiate a hybrid conflict designed to destabilize the Republic of Moldova, exploiting the pro-Russian elements within the society. Moreover, the Russian Armed forces’ presence in Transnistria represents an extreme vulnerability and an ultimate option for Kremlin to start an aggression. Both possibilities will generate extreme security concern for Romania, a country with a unique relationship with the Republic of Moldova, especially as many citizens from the eastern side of the Prut River have Romanian citizenship. Romania has to intervene somehow in any possible conflict affecting its citizens with unpredictable consequences for the country and its allies. From another perspective, the Russian Federation already maintains a high level of control throughout the Moldavian socio-politico-economic environment, probably assessed as sufficient. Also, the Kremlin probably understands that a huge part of the population is western orientated, and is already involved on multiple fronts in Europe and the Middle East, probably preferring to preserve a frozen conflict in Transnistria and its influence over the entire country, rather than escalating a hybrid or conventional conflict with unclear second-order effects.

From the Romanian perspective, the most important security guarantees are enabled by NATO and the Strategic Partnership with the US, materialized in NATO and US troops on the ground. However, under the current leadership, the US has adopted an isolationist agenda with an avalanche of populist statements targeting an internal audience, but directly affecting partners’ trust in the American commitment to NATO. President Donald Trump asked money in return of "*the privilege of hosting US troops*"[22], maintaining a European concern over the US genuine adherence to the Article 5 principle. Moreover, the retreat from the Intermediate-Range Nuclear Forces Treaty brings back Cold-War fears[23], fuelling the European Army project idea or other security cooperation format in case of an "*American abandonment*". For Romania, the scenario of US reducing its involvement in Europe would probably result in major security concerns, in an area with on-going military conflicts and intimidation, without other European security projects comparable with the US military power, proven through the deployments in Kogalniceanu Airbase and the Missile Shield project in Deveselu. As the strategic partnership is strong, with Romania investing in US military technology, an American "*retreat*" from Romania appears doubtful at the moment. However, in the last 4 years, the US leadership had multiple inadvertences with its European counterparts, while in Romania Exxon Mobil intends to sell their parts in the offshore gas project in the Black Sea[24], therefore Romanian decision-makers cannot rule out this scenario in the long term.

In a Black Sea Region dominated by the Russian Federation on one side and NATO on the other, Romania has to rely on its bilateral and NATO partnerships with Turkey. Still, since the National Defence Strategy 2015-2019 was published, the situation has changed significantly in this case. Turkey maintains an uncertain status within the Nord-Atlantic Alliance, after the Russian military equipment acquisition, its bivalent relations with Russia and Iran, and its actions within Syria. For Romania, Turkey's unclear options bring severe maritime security concerns within the Black Sea, but also the threat of a possible division within NATO, which may put under question the viability of the North-Atlantic project overall. Turkey will probably continue to maintain cold relations with NATO, and even colder with the EU allies of NATO, due to the divergent geopolitical views, impossibility to join the EU, and other particular conflicts with Greece, France and others. Even though Romania preserves a very good bilateral cooperation with Turkey, the regional picture is not favourable and could result in divergent actions in the long term, directly affecting Romania's military security.

In the European security environment, Brexit is definitely the most worrying event affecting military security. As the United Kingdom of Great Britain and Northern Ireland (UK), decided to leave the European community, the EU has lost the most powerful military ally. Even though the UK-EU military cooperation will almost certainly continue within NATO and above, the UK has also to compensate for the economic losses generated by Brexit and probably to reduce unnecessary military expenditures. UK's involvement in Eastern Europe, one of the most consistent among NATO European allies, will possibly decrease, while the need for other economic partners could increase relations with Russia, Turkey, or the non-NATO Balkan countries. Therefore, UK may create vulnerabilities for its Eastern European allies, UK's decisions could be influenced by non-NATO states, and in the most dangerous case scenario, could enable UK's tolerance to aggressions on the eastern partner. Moreover, after Brexit France will remain the only EU country with a permanent veto in the UN Security Council (UNSC) and is determined not to hand it over to the European

[22] Leo Shane III, *Trump wants to charge allies extra money for the privilege of hosting US troops*, Military Times, March 8, 2019, https://www.militarytimes.com/news/pentagon-congress/2019/03/08/trump-wants-to-charge-allies-extra-for-the-privilege-of-hosting-us-troops-report/, accessed Feb. 20, 2020.

[23] *America withdraws from the Intermediate-Range Nuclear Forces Treaty*, The Economist, Feb 1st 2019, https://www.economist.com/united-states/2019/02/01/america-withdraws-from-the-intermediate-range-nuclear-forces-treaty, accessed Feb. 20, 2020.

[24] Gary McWilliams, Luiza Ilie, Christian Schmollinger, *Exxon Mobil confirms may exit Romanian offshore gas project*, January 8, 2020, https://www.reuters.com/article/us-romania-energy-exxon/exxon-mobil-confirms-may-exit-romanian-offshore-gas-project-idUSKBN1Z70XP, accessed Feb. 21, 2020.

Block[25;26]. This is specifically dangerous as the UK has manifested a clear anti-Russian agenda, while France was rather balanced, therefore possible harassments or aggressions of the Russian Federation to the Eastern Europe EU states might be tolerated within the UNSC. Still, the UK has always been a vocal enemy of Russia, which will probably result in no major shifts in its Eastern European foreign policy, probably enabling trust in military and diplomatic support for Romania in the long term.

One must also not forget the impact that Brexit will have on NATO-EU relations. Although the North Atlantic Alliance is not to be affected directly by the UK exit from the European Union, its relation with the latter is bound to be affected to a certain degree, nonetheless. From a security perspective, the change is insignificant: the United Kingdom remains militarily involved in NATO and will continue to participate in all NATO missions. However, the United Kingdom represented a major connector between the EU and the United States of America. The British absence from the EU is likely to determine the US to seek another supporter of its interests within the EU member states[27]. Romania, as still one of the junior members of the EU is highly unlikely to play that part. But the question arising is whether, once the supporter found, will its actions be also favourable to Romania's position within the EU? Indirectly, of course.

Due to all these challenges within the 2020 defence environment, Romania's political and military leaders have to update the threats already perceived in 2015, address the newly emerged ones and take positive measures in order to limit the country's vulnerabilities, while increasing its capacity to respond. By analysing the threats based on risks and effects, Romania could prioritize resources in order to counter the menace efficiently (see the analysis tables at the end).

2. The complexity of the non-military threats in 2020

Despite the relevance of military threats to Romania, the contemporary security environment generates multiple other challenges to national security. The 2015-2019 National Defence Strategy focused on military security, covering the non-military domains just by addressing migration and partially the radicalization phenomena, but, as previously mentioned, in accordance with the Copenhagen School economic, politic, societal, and environmental security have to be seriously addressed. Regardless of the environmental domain, which is mainly an internal policy issue, the external threats to Romania come from all the other security domains.

External threats in the economic domain of security

Due to the irreversible Brexit, Romania and the rest of the EU countries will probably face some economic difficulties provoked by the loss of an export market. However, the Romanian economy is not as dependant on the UK market as similar examples in Europe,

[25] *Germany calls for France to give its UN Security Council seat to the EU*, France 24, Issued on: 28.11.2018, https://www.france24.com/en/20181128-paris-france-german-proposal-un-eu-macron-merkel-security-council-nations, accessed Feb. 24, 2020.

[26] Should the EU take France's seat on the UN Security Council?, Euronews, 29.11.2018, https://www.euronews.com/2018/11/29/should-the-eu-take-france-s-seat-on-the-un-security-council, accessed Feb. 24, 2020.

[27] Oana-Elena Brânda, *NATO-EU relations in the aftermath of Brexit*, in Volume of the International Scientific Conference "Strategies XXI. Strategic Changes in Security and International Relations", Vol. 2, Bucharest, UNAP Publishing House, 2017, p. 78, https://www.strategii21.ro/A/2017-04.%20STRATEGIC%20CHANGES%20IN%20SECURITY%20AND%20INTERNATIONAL%20RELATIONS/VOL%202%20Strategic%20changes%20in%20security%20and%20international%20relations%202017.pdf, accessed at Feb. 26, 2020.

particularly Germany[28] or the countries on the border of the English Channel[29], Brexit not representing a milestone in the current economic growth.

A secondary economic threat after 2020 could be a possible economic migration putting pressure on the Romanian economy, due to UK diaspora that might have to return home or to move within the EU borders. The reality is that a potential economic migration is likely to be absorbed by the on-going human resources crisis within the EU and Romania, without representing a significant problem for the national authorities.

External threats in the societal domain of security

First of all, as mentioned in the National Defence Strategy 2015-2019, migration was a key aspect assessed by Romania from the societal perspective. However, the massive migration phenomenon in 2014-2015 affected just marginally the country, which is not a member of the Schengen Area.

The most common societal threat within the last European decade was populism, with a large representation within the political environment and significant impact on societal security. Populism is one of the key modern drivers of extremism, which after 2020 could increase especially if populist politicians exploit the expected socio-economic problems, trying to explain them by attributing the guilt to some social groups. This phenomenon is probably the most dangerous threat to the post World War European society, governed by tolerance and multiculturalism, and will likely to be fuelled by economic difficulties. For Romania, the general spread of populism and extremism is a key threat to national security, due to their possible impact on the EU cohesion in the long term. Moreover, due to the large Romanian diaspora, extremism might directly target Romanian citizens temporarily residing within Western Europe. The success of political parties like "*Front National*" or "*Fratelli D'Italia*", with pure populist-nationalist agendas, and the recent examples of extremist activity in Germany[30;31] prove that the European society is at a crossroad, forcing the Romanian authorities to seriously assess the phenomenon in order to act for in support of a strong multicultural EU that will protect the rights of its citizens at home and abroad.

From a different perspective, after Brexit, the European authorities backed French and German leaders will probably try to accelerate the integration process[32], more likely within the economic, financial and politico-military domains, taking advantage of the favourable context. Without the UK, a traditional voice opposing the EU federalisation, and with the need for stability and a strongly united European block, EU might try to force a more cohesive union, homogenous or with multiple speeds, overpassing the basic principle of "*unity in diversity*". Romania as most of the other countries must analyse this scenario, allocating diplomatic resources to avoid any potential significant socio-cultural damage with a major impact on the national identity in the long term.

[28] Wolfgang Münchau, *Why German industry should fear a no-deal Brexit*, Finacial Times, 24.06.2018, https://www.ft.com/content/c06b1762-761d-11e8-b326-75a27d27ea5f, accessed Feb. 24, 2020.

[29] Alessandra Scotto di Santolo, *EU to hold UK to ransom over fishing waters to get Brexit deal done by summer*, Express, Tue, Jan 21, 2020, https://www.express.co.uk/news/uk/1231190/brexit-news-uk-eu-trade-deal-uk-fishing-waters-eu27-gavin-barwell, accessed Feb. 24, 2020.

[30] *Germany shooting: 'It was a shock but not a surprise'*, BBC, 20.02.2020 https://www.bbc.com/news/world-europe-51576446, accessed on Feb. 23, 2020.

[31] *Germany shooting: chants of 'Nazis out' at vigils after gunman kills nine*, The Guardian, 21.02.2019, https://www.theguardian.com/world/2020/feb/21/germany-shooting-chants-of-nazis-out-at-vigils-after-gunman-kills-nine, accessed on Feb. 23, 2020.

[32] *Ursula von der Leyen and the Shape of Post-Brexit Europe*, Guild Investment Management, Equities, 28 October 2019, https://www.equities.com/news/ursula-von-der-leyen-and-the-shape-of-post-Brexit-europe, accessed on Feb. 23, 2020.

In addition to the mostly abstract threats to the Romanian society and culture, a possible pandemic menace has to be taken into account, as a primary hazard that may affect the society, economy and overall security. In the middle of the COVID19 epidemic, highly likely to end with severe casualties and economic losses, and with the on-going world connectivity and mass migration, the pandemic threat should be actively monitored and contingency plans and resources should be carefully prepared in order to avoid any significant effects for the Romanian society.

External threats in the political domain of security

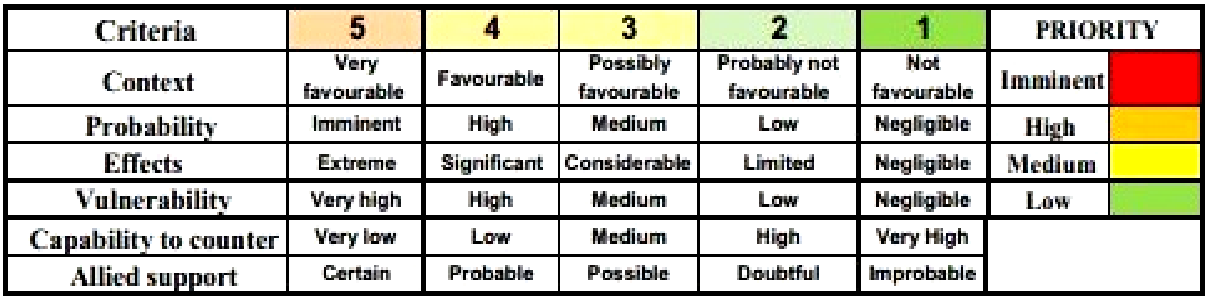
From the political perspective, the current post-Brexit instability, combined with populism across the EU might result in a very dangerous course of action involving other EXITs. This is still a low-probability scenario, but in case of other states' decision to leave the European community, the domino effect is likely to generate a major threat to Romania, whose political-economic stability and prosperity depends on a strong EU.

Regarding the political integration within the EU, an acceleration of the integration process, especially in the case of the multiple speed option is likely to bring EU internal divisions, due to the opposition of individual countries including Romania, or associations of states such as the Visegrad Group. Romania has to identify this scenario and act individually or in coalitions to protect its interest, providing a significant argument for a homogenous and economically-stable EU.

3. In place of conclusions: External threats assessment – Romanian priorities

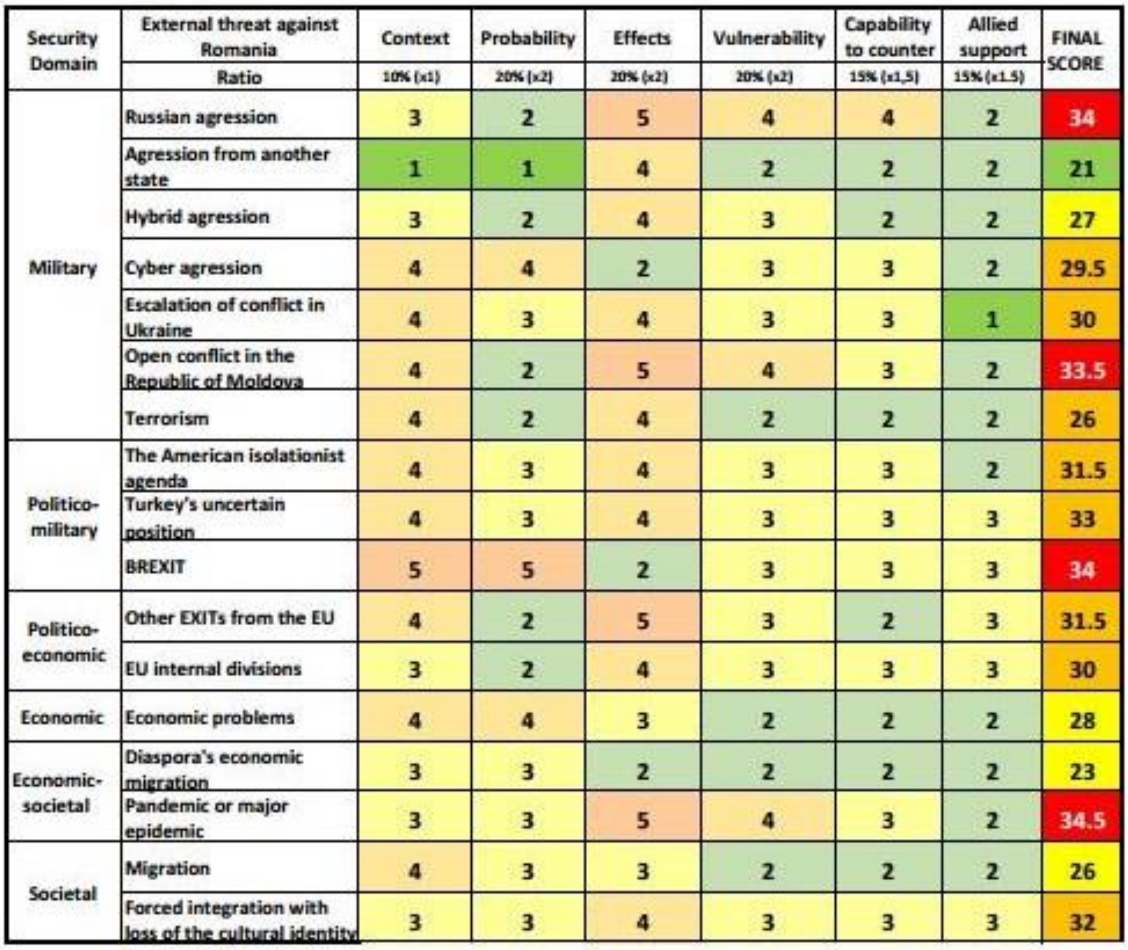
All the previously mentioned threats represent key aspects to be included in future Romanian security strategies. In order to try to determine their priority for the Romanian authorities, the analysis will compare them based on six criteria, with different ratios, context (10%), probability (20%), effects in the long term (including magnitude, 20%), vulnerability to the threat (20%), capability to counter (15%), and the potential support from the allies in NATO and EU (15%). The final score of every threat will determine if the menace is of imminent priority (over 33), high priority (28.5 to 33), medium priority (22 to 28) or low priority (under 22). The security domain will be analysed taking on spot external threat against Romania including military, politico-military, politico-economic, economic, economic-societal and societal.

Table 1. Criteria and priority table



Criteria	5	4	3	2	1	PRIORITY	
Context	Very favourable	Favourable	Possibly favourable	Probably not favourable	Not favourable	Imminent	🟥
Probability	Imminent	High	Medium	Low	Negligible	High	🟧
Effects	Extreme	Significant	Considerable	Limited	Negligible	Medium	🟨
Vulnerability	Very high	High	Medium	Low	Negligible	Low	🟩
Capability to counter	Very low	Low	Medium	High	Very High		
Allied support	Certain	Probable	Possible	Doubtful	Improbable		

Table 2. The analysis of external threats against Romania



Security Domain	External threat against Romania	Context	Probability	Effects	Vulnerability	Capability to counter	Allied support	FINAL SCORE
	Ratio	10% (x1)	20% (x2)	20% (x2)	20% (x2)	15% (x1,5)	15% (x1.5)	
Military	Russian agression	3	2	5	4	4	2	34
	Agression from another state	1	1	4	2	2	2	21
	Hybrid agression	3	2	4	3	2	2	27
	Cyber agression	4	4	2	3	3	2	29.5
	Escalation of conflict in Ukraine	4	3	4	3	3	1	30
	Open conflict in the Republic of Moldova	4	2	5	4	3	2	33.5
	Terrorism	4	2	4	2	2	2	26
Politico-military	The American isolationist agenda	4	3	4	3	3	2	31.5
	Turkey's uncertain position	4	3	4	3	3	3	33
	BREXIT	5	5	2	3	3	3	34
Politico-economic	Other EXITs from the EU	4	2	5	3	2	3	31.5
	EU internal divisions	3	2	4	3	3	3	30
Economic	Economic problems	4	4	3	2	2	2	28
Economic-societal	Diaspora's economic migration	3	3	2	2	2	2	23
	Pandemic or major epidemic	3	3	5	4	3	2	34.5
Societal	Migration	4	3	3	2	2	2	26
	Forced integration with loss of the cultural identity	3	3	4	3	3	3	32

The comparative analysis identifies potential priorities for Romania within various security domains. First of all, the analysis shows the already acknowledged threat posed by the Russian Federation, but the Romanian authorities have to assess the comprehensive military security environment, addressing the potential Russian aggressions also against key partners, especially the Republic of Moldova. Moreover, Romania has to shift its defence-based strategy into a more complex security strategy as unpredictable changes such as Brexit, with impact over the political, economic, military and societal domains, or a major epidemic threat like COVID 19 corroborated with the globalisation and massive human movement, are events not covered by the on-going national defence strategy.

From a bigger picture point of view, Romanian political and security specialists need to agree with the idea that the threats are not individual, but rather complementary. For example, Brexit, a country's decision of leaving a political-economic alliance, could affect the military security in Eastern Europe, societal problems around Europe and trigger other EXIT political-economic threats. Another example could be Turkey's unclear path, with multiple divergent opinions related with the EU and the migration blackmail. Turkey's political decisions might weaken NATO-Russian balance within the Black Sea Region, but also by allowing a major migration wave, combined with the possible economic problems after Brexit, and the menace of an uncontrolled epidemic threat, could enable European instability. Furthermore, an EU internal instability in the long term will enable forced integration, posing a threat to the national cultures, or will aggravate EU divisions and isolationism, enable populism and extremism, or, in the most dangerous scenario trigger a domino EXIT phenomenon ending the European project.

As a general perspective, the 2020 security environment is characterized by complexity, volatility and unpredictability, the last decade historical analysis proving that most of the current threats to Europe and Romania were marginally predicted. For Romania, the legal need for a new national strategy after the 2019 presidential elections represents an opportunity for subject matter experts to recommend the shift toward a National Security Strategy 2020-2024. This document could provide the framework for a more comprehensive approach toward the current security challenges, without the limitations of the term "*defence*", which usually is attributed to military security. Despite the obvious military security threats, Romania has to address the imminent priorities like Brexit and the COVID 19 epidemic, with a high probability to turn into a pandemic threat. In addition to the conversion into a security strategy, Romania has to think about a long-term document to address this field in order to project its military, economic, including energetic, political, societal and environmental security interests for at least 10 years, with legal possibilities to update it due to major shifts within the environment, rather than internal elections.

BIBLIOGRAPHY

1. Bulgarian National Assembly, National Security Strategy of the Republic of Bulgaria, 2011;
2. Estonian Ministry of Defence, National Defence Strategy Estonia, 2011;
3. Romanian National Government, *Cyber Security Strategy of Romania*, 2013;
4. Seimas of the Republic of Lithuania, The National Security Strategy, Resolution No XIII-202, 2017;
5. The Republic of Latvia, The National Security Concept (informative section) https://www.mod.gov.lv/sites/mod/files/document/NDK_ENG_final.pdf
6. The President of Poland, The National Security Strategy of The Republic of Poland, 2014;
7. United Nations, *Charter of the United Nations and Statute of the International Court of Justice*, Chapter V., San Francisco, 1945;
8. University of Cambridge, *Cambridge Dictionary*, 2018, Cyber warfare definition, https://dictionary.cambridge.org/dictionary/english/cyber-warfare
9. Emma Beswick, *Which countries spend the most on their military?*, last updated: 02/05/2018, EuroNews, https://www.euronews.com/2018/05/02/which-country-spent-the-most-on-its-military-in-2017-
10. Oana-Elena Brânda, *NATO-EU relations in the aftermath of Brexit*, in Volume of the International Scientific Conference "Strategies XXI. Strategic Changes in Security and International Relations", Vol. 2, Bucharest, "Carol I" National Defence University Publishing House, 2017, pp. 75-83, https://www.strategii21.ro/A/2017-04.%20STRATEGIC%20CHANGES%20IN%20SECURITY%20AND%20INTERNATIONAL%20RELATIONS/VOL%202%20Strategic%20changes%20in%20security%20and%20international%20relations%202017.pdf
11. Oana-Elena Brânda, *The Three-Seas Initiative – A New Role for Romania?*" Proceedings of the International Conference "Defence Resources Management in the 21st century", Brașov, "Carol I" National Defence University Publishing House, 2018, pp. 83-90, http://www.codrm.eu/conferences/2018/Carte%20CoDRM%202018.pdf
12. Vilém Kolín, *The Role of War in International Politics*, Úloha Války V Mezinárodní Politice, https://www.obranaastrategie.cz/filemanager/files/6265-en.pdf

13. Nikolas K. Gvosdev, The Bear Awakens: Russia's Military Is Back, The National Interest, November 12, 2014, https://nationalinterest.org/commentary/russias-military-back-9181
14. Fenella McGerty, *Jane's Defence Budgets - Global Budgets Trends*, Jane's Defence, 13 March 2018, https://www.janes.com/article/78514/jane-s-defence-budgets-global-budgets-trends-2018
15. Gary McWilliams, Luiza Ilie, Christian Schmollinger, *Exxon Mobil confirms may exit Romanian offshore gas project*, January 8, 2020, https://www.reuters.com/article/us-romania-energy-exxon/exxon-mobil-confirms-may-exit-romanian-offshore-gas-project-idUSKBN1Z70XP
16. Bret Perry, *Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations*, Small War's Journal, https://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera
17. Max Roser, Mohamed Nagdy, *Military Spending, Empirical View*, Our world Data, https://ourworldindata.org/military-spending
18. Alessandra Scotto di Santolo, *EU to hold UK to ransom over fishing waters to get Brexit deal done by summer*, Express, Tue, Jan 21, 2020, https://www.express.co.uk/news/uk/1231190/brexit-news-uk-eu-trade-deal-uk-fishing-waters-eu27-gavin-barwell
19. Leo Shane III, *Trump wants to charge allies extra money for the privilege of hosting US troops*, Military Times, March 8, 2019, https://www.militarytimes.com/news/pentagon-congress/2019/03/08/trump-wants-to-charge-allies-extra-for-the-privilege-of-hosting-us-troops-report/
20. Wolfgang Münchau, *Why German industry should fear a no-deal Brexit* , Finacial Times, 24.06.2018, https://www.ft.com/content/c06b1762-761d-11e8-b326-75a27d27ea5f
21. *America withdraws from the Intermediate-Range Nuclear Forces Treaty*, The Economist, Feb 1st 2019, https://www.economist.com/united-states/2019/02/01/america-withdraws-from-the-intermediate-range-nuclear-forces-treaty
22. *Germany calls for France to give its UN Security Council seat to the EU*, France 24, Issued on: 28.11.2018, https://www.france24.com/en/20181128-paris-france-german-proposal-un-eu-macron-merkel-security-council-nations
23. *Germany shooting: 'It was a shock but not a surprise'*, BBC, 20.02.2020, https://www.bbc.com/news/world-europe-51576446
24. Germany shooting: chants of 'Nazis out' at vigils after gunman kills nine, The Guardian, 21.02.2019, https://www.theguardian.com/world/2020/feb/21/germany-shooting-chants-of-nazis-out-at-vigils-after-gunman-kills-nine
25. *NATO's response to hybrid threats*, Last updated: 08 Aug. 2019, https://www.nato.int/cps/en/natohq/topics_156338.htm
26. *Pactul pentru Apărare a fost semnat. Președintele: Este un acord implicit pentru dezvoltarea industriei naționale de apărare*, 13.01.2015, https://www.digi24.ro/stiri/actualitate/politica/pactul-pentru-aparare-a-fost-semnat-presedintele-este-un-acord-implicit-pentru-dezvoltarea-industriei-nationale-de-aparare-346358

27. *Should the EU take France's seat on the UN Security Council?*, Euronews, 29.11.2018, https://www.euronews.com/2018/11/29/should-the-eu-take-france-s-seat-on-the-un-security-council
28. *Ursula von der Leyen and the Shape of Post-Brexit Europe*, Guild Investment Management, Equities, 28 October 2019, https://www.equities.com/news/ursula-von-der-leyen-and-the-shape-of-post-Brexit-europe
29. https://www.sri.ro/cyberint
30. https://cert.ro/
31. https://www.cybercommand.ro/

THE ENVIRONMENTAL CONFLICT: ONE OF THE DISRUPTIVE NON-MILITARY FACTORS OF WORLDWIDE SECURITY

Claudia Clara ALEXE (ȘTIRBU)
Dr. Eng., Student of the master's program ”Crisis management and conflict prevention”-
National Defence University “Carol I”
stirbuclaudiaclara@gmail.com

Abstract*: Since life originated on Earth, the environment has represented a necessity, an objective and a right, which was often earned by force. The fight for survival had led to the first forms of migration to areas which offered favourable/adequate living conditions with productive soils, water sources, lush flora and fauna. Therefore, it was a fight for access to natural resources. This is why we can say the first conflicts were environmental, generating military conflicts. The concept of environmental conflict had appeared in the last 50 years, but it seems to have been the basis of the other types of conflict (political, administrative, social, economic, ethnic and cultural).*

Keywords*: climate, human, conflict, security.*

Introduction

We can sketch a triangle of triggering factors of the environmental conflict, which are characterized by connectivity and interdependence, and target both environmental conditions (the ecological sphere), as well as the social and economic sphere. Depending on the interconnections between these three points, a series of threats and risks can be outlined which will be the basis of a conflict that may have a cyclical character or which can be considered in dynamics, being practically visible the “*chronic*” aspect of the environmental conflicts.

When the social sphere is under the influence of rapid demographic growth, in a fragile or unstable socio-political, educational environment, the first reflections that appear are in the economic sphere, this being the direct cause of the appearance of the imbalance in the living environment.

At this point we begin to discuss the anthropic factor - as a disruptive factor, the human being carrying out at any given moment, any type of activity that can ensure immediate economic stability, giving him the fragile image of the sustainability of the created living environment and the illusion of a state of security. When I say “*human being*” - I make clear reference both to the individual, as the link of society and to society - as a whole, made up of a group of individuals who have common goals and strategies and policies aimed at achieving them. Thus, a series of conflicts can arise which are based on the way of managing the resources - these can generate territorial-administrative conflicts, or in economic-socio-environmental conflicts, which concern the whole process of sustainable development. As a result, the anthropic factor represents the oldest and most persistent threat to the environment, in general and to climate conflict in particular.

Today, the environmental conflict is a factual state, based on the conflict between two or more actors involved; one party challenging the way the other involved party ignores or acts against policies and measures that ensure a sustainable environment.

The role of the anthropic factor in the dynamics of the environmental conflict

At present, the environmental conflict does not only manifest itself in a certain time, between two or more parts of a dispute aimed at obtaining natural resources or better environmental conditions, but we can also speak of an environmental conflict between generations, a concept that imposes an increasingly important place in the classification of conflict typology. This conflict seems to be of an emotional, psychological type, unfolding with a permanent character, through a portal that gives us a desolate image, of a poor planet, with a population affected by congenital diseases, genetic mutations or simply not adapted to environmental conditions. The psycho-emotional segment can be easily used as a "*weapon*" in political development strategies, but like any weapon, it can be used for both defence and attack. In the following figure we tried to summarize the scenario regarding the dynamics of the environmental conflict and the importance of the role played by the anthropic factor.

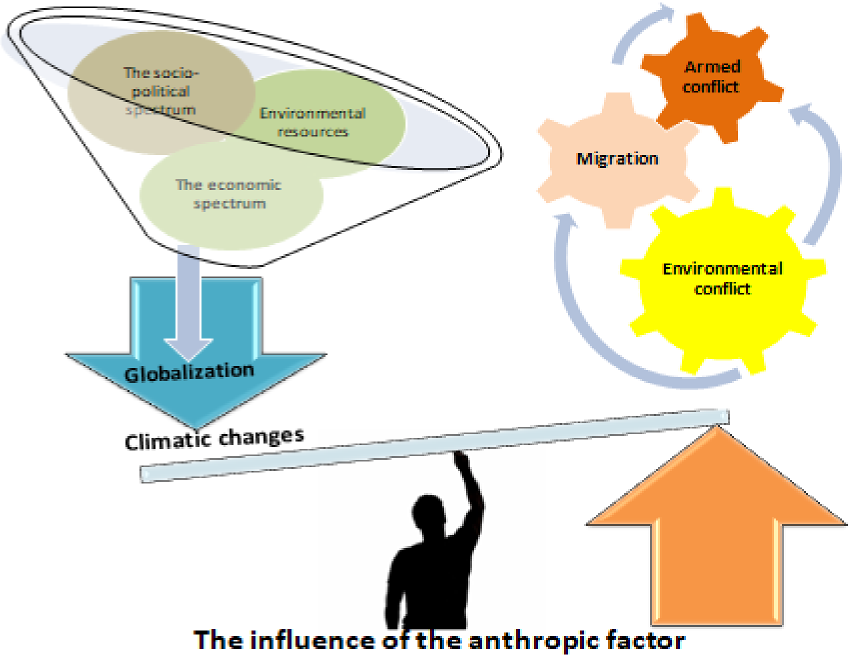


Fig. 1 The role of the anthropic factor in the dynamics of the environmental conflict

Why did I point out that one of the most disturbing non-military factors in world security is the environmental conflict? The great discoveries, but also the great conflicts started from the need to provide resources, thus, the discovery of the Indies, the discovery of America are examples of critical moments of the demographic dynamics and especially of the migration phenomenon. Migration to America reached its highest levels after the Second World War, when it was considered a real refugee crisis. In the post-1970 period, America remained the main attraction of international migrants, but in 2015 Europe faced the worst refugee crisis after the Second World War, and in a single year, the EU member states to grant asylum to over 700,000 refugees. According to data presented in the European Commission Report in 2016, the EU has more than three times the number of refugees registered in Australia, Canada and the United States together in that year.

The data presented raised the issue of ensuring regional security and the environmental conflict with the international impact.

The USA, since 1996, has emphasized the existence in the category of non-military risks "*of stringent problems regarding natural resources and transnational environmental issues*", being considered an important asset in the US Security Strategy, being established the first analysis offices of ecological and environmental issues at the level of the State Department and the National Security Council.

The global warming phenomenon has started to create concerns since 1960, when, as a result of the large-scale development of the industrial sector and its effects, mainly referring to the increase of the concentration of greenhouse gases, these being considered as the main trigger factor and accelerator of this phenomenon. Following the studies, the statistical processing of the existing data and the use of mathematical models for estimating climate change, the specialists in the field estimate a variation of the phenomenon of climate warming, which will be based on temperature increases of 1.1°C up to 6,4°C throughout the century[1], scenarios that place a special emphasis on polar areas, which, it seems, will warm up the most, the consequences being estimated to be dramatic.

The global warming phenomenon has been strongly felt over the last two years, producing devastating effects for some regions. In 2016, in India there was a temperature record, in the area of Phalodi city - a region of northern India, with a very high population density, which could barely stand to the recorded 51°C[2]. Excessive heat caused hundreds of deaths in a few days, drought affecting agriculture in 13 Indian states and displacement of tens of thousands of locals. According to the same sources, the ocean currents have changed their direction under the influence of the global temperature rise, the result having an effect on the melting of glaciers. And in 2017, in the Balkans area, a high percentage of deaths were registered, as a result of the "*Lucifer*" heat wave. The years 2018 and 2019 were in turn, considered the warmest and driest years for northern Europe.

In the article *"Europe warms up and shows no signs of cooling in the near future*", the European Data Journalism Network (EDJNet)[3] published the results of research on the evolution of the climate warming phenomenon in Europe, stressing that the most affected areas are Andalusia and the south-east area of Romania, where temperatures have risen by 1.6 and 1.5^{0}C more than those registered in the last century, respectively. This period of accelerated growth of global warming, coupled with the impact of the anthropic factor, leads to a considerable diminution of water sources worldwide.

The European Union also takes care of the vulnerabilities of the neighbouring regions, bearing in mind the fact that in order to maintain a state of peace and security within the EU, inter-regional stability is needed. History has shown that the lack of water can affect peace and security, as well as being able to generate significant human and economic costs and implicitly a series of direct implications for the EU, the most frequent being the change of migration flows.

In the Joint Communication to the European Parliament and the Council, held in May 2019 on the topic "*European Union and Central Asia: new opportunities for a stronger partnership*", the situation of Central Asia has been emphasized from the beginning, which "*is facing greater and greater challenges in the environmental field. The combined impact of climate change, which has begun to reduce the flow of water by reducing the glaciers that feed Central Asia's rivers and the rapid population growth, will exacerbate some of the region's environmental problems, generating potential implications for economic development, security and migration.*"[4]

Throughout human evolution, the source of water has been decisive in establishing and developing habitats, as the need for water and food is often a source of conflict of all kinds, including armies. The way in which "*the human being*" has managed the water sources over time, have led to imbalances of the ecosystems and implicitly to the local social conflicts, which have often had an amplification of the effects at regional level. One such

[1] *Lupta împotriva schimbărilor climatice*, ONU Conference, Paris, 2015, https://www.europarl.europa.eu/factsheets/ro/sheet/72/lupta-impotriva-schimbarilor-climatice accessed Feb. 15, 2020.

[2] Oraan Mărculescu, *Încălzirea globală e mai rapidă decât s-a estimat*, Revista Știință și tehnică, 8 iunie 2017. https://stiintasitehnica.com/incalzire-globala-rapida/ accessed Feb. 15, 2020.

[3] European Data Journalism Network, *Europa se încălzește și nu arată niciun semn de răcire în viitorul apropiat*, (article translated by Claudiu Pop), https://voxeurop.eu/ro/2019/nc-lzire-global-5124127 accessed Feb. 15, 2020.

[4] Comunicare comună către Parlamentul European și Consiliu, *Uniunea Europeană și Asia Centrală: noi oportunități pentru un parteneriat mai puternic*, Bruxelles, May 15, 2019

example is the drying of the entire Aral Sea, considered in the past one of the largest lakes in the world, and which had to suffer with the start, in 1960, of large hydro technical works that changed the course of two large rivers, Syr Darya and Amu Darya pouring into the lower basin of the Aral Sea[5]. The purpose of this grand project was strictly related to the need for water supply of the Kyzylkum desert area, which was to become an area with favourable living conditions. Since 1960, the surface of the Aral Sea has changed from year to year, especially during the droughty years like 2005-2009. In 2014, the sea dried up completely, and the population of the area migrated, being on the one hand forced by job losses - most being fishermen, and on the other hand, the security of the region was affected. Everything turned into a desert in which a full air of toxic dust was inhaled as a result of contamination with salts, fertilizers and remaining pesticides.

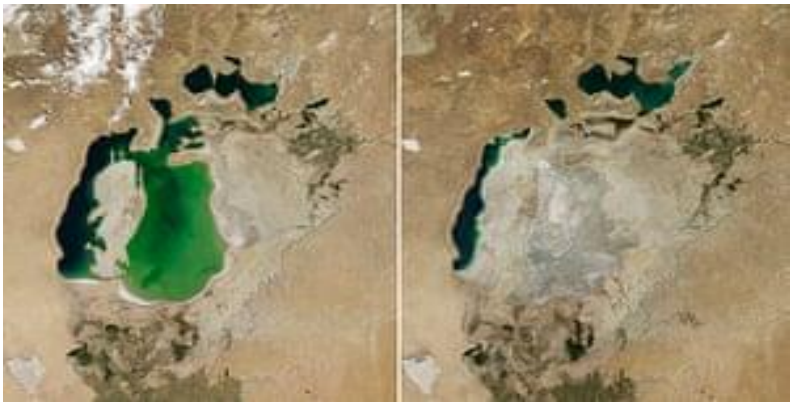


Fig. 1 The Aral Sea in 2000 on the left and 2014 on the right. Photograph: Atlas Photo Archive/NASA[6]

And the largest freshwater lake in the world, Lake Baikal, which was considered to represent almost a quarter of the world's freshwater reserve, was placed in 2016 on a "*list*" of potential ecological disasters due to the anthropic factor and stimulated by the effects of global warming. And in this case, the trigger factor is people's desire to ensure good living conditions, without analysing the long-term effects. Mongolia has proposed and started a grandiose project to build a chain of hydroelectric power stations and dams along the Selenga River and its tributaries, a river that completes its course in Lake Baikal. A member of the Russian parliament, Oleg Lebedev, said that these interventions lead to limiting access '*to freshwater, which was already difficult, of inhabitants of the regions of Buryatia and Irkutsk"*, with studies showing that the lake level is already low, the effect being felt at only 300 km away, where the wells have already dried[7]. This case was treated in 2016 as a Russian-Mongolian political-economic conflict, but it can be categorized as a real environmental conflict, characterized by a series of variables, of political, economic and social order, which highlight the vulnerabilities of any state in the occurrence of an induced ecological risk.

[5] Nicu Pârlog, *Cazul Aral: o mare în moarte clinică*, 01.09.2013, https://www.descopera.ro/natura/10439989-cazul-aral-o-mare-in-moarte-clinica accessed Feb. 15, 2020.

[6] Enjoli Liston, *Satellite images show Aral Sea basin 'completely dried'*, 1 Oct. 2014 https://www.theguardian.com/world/2014/oct/01/satellite-images-show-aral-sea-basin-completely-dried?CMP=fb_gu) accessed Feb. 15, 2020.

[7] Adrian Nicolae, *Lacul Baikal riscă să dispară asemenea mării Aral*, Știință și Tehnică, 03.06.2016, https://stiintasitehnica.com/lacul-baikal-risca-sa-dispara-asemenea-marii-aral/ accessed Feb. 15, 2020.

An alarm signal is being fired by environmental activists from Azerbaijan[8] *and the* Caspian Sea, who are facing a situation that is compared by specialists with that of the Aral Sea, rapidly lowering the water level, and the marine biodiversity is severely affected.

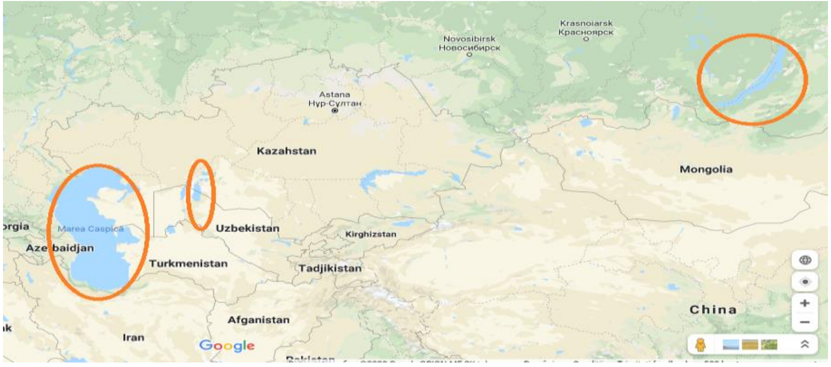


Fig. 2 Areas of Central Asia with environmental and socio-economic imbalances as a result of climate change under the direct influence of the anthropic factor

These are just a few of the situations identified in the Central Asia area that are, under the impact of the anthropic factor and climate change, or can become anytime, triggering factors of environmental conflicts, which as a result of the ecosystem imbalances, can culminate with the severe reduction of vital resources, and implicitly in migratory waves or the emergence of pandemics.

Considered to be multipliers of threats to the security of nations, climate change and the effects of environmental degradation, they will be the subject of conversations of representatives of EU and Central Asian countries on policies and actions to prevent conflict, humanitarian and development actions, as well as reduction strategies of disaster risks throughout Central Asia.

Conclusions

Within the global strategy for the European Union's foreign and security policy, three priorities are aimed at strengthening partnerships with Central Asian countries in order to increase resilience, namely: partnerships for resilience, prosperity and better collaboration. The ability to anticipate and address the challenges affecting the socio-economic objectives and security of these countries will be considered, in order to strengthen their capacity to carry out new reforms in vulnerable sectors. The partnerships will have as basic principles democracy, human rights and the rule of law, stimulating cooperation on the implementation of the Paris commitments on climate change and addressing trans regional environmental challenges, *"to turn them into opportunities and increase cooperation on migration.”*[9]

Related to the strategy of the European Union, the increase of the resilience of Central Asia is a major interest, but which, as we have pointed out, requires a strengthening of the capacity of the component countries, *"to anticipate and resist external and internal pressures, to adopt reforms and to address the challenges generated by globalization, rapid population growth, climate change, environmental degradation, pressure on water and energy resources, labor migration and new security threats.”*[10]

[8] Ilinca Dragoş, *Marea Caspică este în pericol!*, Evenimentul zilei, 01.05.2019, https://evz.ro/marea-caspica-soarta-marea-aral.html accessed Feb. 15, 2020.

[9] Comunicare comună către Parlamentul European și Consiliu, *Uniunea Europeană și Asia Centrală: noi oportunități pentru un parteneriat mai puternic*, Bruxelles, 15.5.2019, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2019:0009:FIN:RO:PDF) accessed Feb. 15, 2020.

[10] *Ibidem*, p. 3.

In November 2018, the working meetings of the members of the EU Council on water diplomacy[11] took place, and the conclusions presented emphasized the need for a regional promotion of an agenda for water, peace and prosperity, being considered a priority for increasing regional resilience. To this end, mutually acceptable solutions to improve regional cooperation relations and fair management of cross-border water resources will be encouraged. The agenda provides for permanent collaboration with relevant UN agencies[12] and with state and non-state partners, encouraging cooperation around the Aral Sea, as well as the implementation of the Agreement on the legal status of the Caspian Sea[13].

Also, the General Congress of the United Nations declared the years 2018-2028 "International Decade of Action - Water for Sustainable Development", which began with the marking of the World Water Day last year, 2018. "We leave no one behind" , it was titled the central theme of the 2019 edition of World Water Day and at the same time the central promise of the 2030 Agenda adopted by the United Nations in 2015, which set the goals of sustainable development of humanity for the period 2015-2030. The 6th Sustainable Development Goal (SDG) is the one that proposes that the entire population of the planet have access to quality water resources by 2030, including objectives on the protection of the natural environment and reducing pollution. From the statistical data presented by the UN, alarm signals can be highlighted regarding the effects of acute water shortages, which by 2030 could cause the migration (displacement) of over 700 million people worldwide[14].

BIBLIOGRAPHY

1. European Data Journalism Network, *Europa se încălzește și nu arată niciun semn de răcire în viitorul apropiat,* (article translated by Claudiu Pop), https://voxeurop.eu/ro/2019/nc-lzire-global-5124127
2. Ilinca Dragoș, *Marea Caspică este în pericol!*, Evenimentul zilei, 01.05.2019, https://evz.ro/marea-caspica-soarta-marea-aral.html
3. Enjoli Liston, Satellite images show Aral Sea basin 'completely dried', 1 Oct. 2014 https://www.theguardian.com/world/2014/oct/01/satellite-images-show-aral-sea-basin-completely-dried?CMP=fb_gu)
4. Oraan Mărculescu, *Încălzirea globală e mai rapidă decât s-a estimat*, Revista Știință și tehnică, 8 iunie 2017, https://stiintasitehnica.com/incalzire-globala-rapida/
5. Adrian Nicolae, *Lacul Baikal riscă să dispară asemenea mării Aral*, Știință și Tehnică, 03.06.2016, https://stiintasitehnica.com/lacul-baikal-risca-sa-dispara-asemenea-marii-aral/
6. Nicu Pârlog, *Cazul Aral: o mare în moarte clinică*, 01.09.2013, https://www.descopera.ro/natura/10439989-cazul-aral-o-mare-in-moarte-clinica
7. Comunicare comună către Parlamentul European şi Consiliu, *Uniunea Europeană și Asia Centrală: noi oportunități pentru un parteneriat mai puternic,* Bruxelles, 15.05.2019, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2019:0009:FIN:RO:PDF)
8. Convention on the Protection and Use of Transboundary Watercourses and International Lakes, concluded at Helsinki on 17 March 1992, https://lege5.ro/Gratuit/gy2temzz/conventia-privind-protectia-si-utilizarea-cursurilor-de-apa-transfrontiere-si-a-lacurilor-internationale-din-17031992

[11] *Diplomația în domeniul apei – Concluziile Consiliului*, 13991/18, 19 noiembrie 2018, https://data.consilium.europa.eu/doc/document/ST-13991-2018-INIT/ro/pdf) accessed Feb. 15, 2020.

[12] Convention on the Protection and Use of Transboundary Watercourses and International Lakes, concluded at Helsinki on 17 March 1992.

[13] Signed on August 12, 2018 at Aktau.

[14] *Lipsa apei curate, un pericol mai mare decât conflictele armate*, Ziarul Bursa, 25.03.2019, https://www.bursa.ro/lipsa-apei-curate-un-pericol-mai-mare-decat-conflictele-armate-42137632 accessed Feb. 15, 2020.

9. *Diplomația în domeniul apei* – Concluziile Consiliului, 13991/18, 19 noiembrie 2018, https://data.consilium.europa.eu/doc/document/ST-13991-2018-INIT/ro/pdf
10. *Lipsa apei curate, un pericol mai mare decât conflictele armate*, Ziarul Bursa, 25.03.2019, https://www.bursa.ro/lipsa-apei-curate-un-pericol-mai-mare-decat-conflictele-armate-42137632
11. *Lupta împotriva schimbărilor climatice*, ONU Conference, Paris, 2015, https://www.europarl.europa.eu/factsheets/ro/sheet/72/lupta-impotriva-schimbarilor-climatic

A EURO-ATLANTIC PERSPECTIVE ON COUNTERACTING THE HYBRID THREAT

Viorel BARBU
Colonel, Ph.D. Candidate, Ministry of National Defence, Bucharest, Romania
viorel_barbu_map@yahoo.com

Abstract: *The new security environment has undergone major transformations, and actors who must counteract hybrid aggression are trying to adapt to the new reality. Through its wide applicability, the modern - hybrid - conflict has repercussions in almost all areas of activity of a nation, its harmful consequences manifesting both in the civilian life and in the military environment. From this perspective, studying hybrid actions is essential for establishing the most appropriate directions and paths of action, as well as choosing the most effective methods and means against hybrid aggression. Thus, actions aimed at counteracting hybrid threats are part of a larger register, covered under the heading of crisis management, with aspects which are debated in the specialized military literature. NATO, like the international community, first came into contact with the hybridity of the modern conflict in March 2014, when it appeared that the Alliance was taken by surprise by the emergence, out of nowhere, of "little green men" without military insignia, but well armed, who proceeded to block and occupy, over the next few days, the main military and political strategic sites of the Crimean Peninsula. As a result, the efforts of the EU and NATO, as political-military organizations, as well as individual Member States, focus on the development of various Armed Forces, in training and materiel, to execute actions specific to the new type of conflict. They also try to augment the overall readiness levels of society by increasing the resilience of people and institutions to hybrid risks, vulnerabilities and threats.*

Keywords: *security environment, hybrid threats, risks and vulnerabilities, counteraction, resilience.*

Introduction

At the beginning of this millennium, the security environment registered major changes from a conceptual point of view, in particular through the emergence of hybrid conflicts. As a result, defence actors are also trying to adapt to the new reality, having to identify and counteract hybrid threats and aggressions. However, although the physiognomy of the wars has undergone major changes, the participants in the conflict still resort to violent, purely military actions.

From this perspective, the study of the hybrid conflict and of the transformations that this type of war brings in the foreground is essential for establishing the most suitable directions and paths of action and choosing the most effective methods and means against hybrid aggression. By its wide applicability, the modern hybrid conflict has implications in almost all fields of activity of a nation, its harmful consequences manifesting both in civilian life and in the military environment. Because of the effects it produces, which are usually determinating factors for the political-military decision-making structures of a state, the real problem from the perspective of hybrid threats is not only understanding the phenomenon, but also identifying solutions to counteract this type of threat.

NATO, like the entire international community, first encountered the hybrid warfare concept in March 2014, and in the beginning, the Alliance appeared to be totally surprised by the sudden emergence of *little green men*, without military insignia but well-armed and who blocked and occupied in a few days the main military and political strategic objectives of the Crimean Peninsula.

In the fall of the same year, at the NATO Summit in Wales (September 4-5, 2014), Robert G. Bell, the civilian representative of the US Secretary of Defence in Europe and the US ambassador for defence in NATO, supported the inclusion of hybrid conflict on the agenda of the reunion and based his proposal on the conclusions of the analysis of the conflict in Ukraine: “*Which can be described as asymmetrical, of unassigned aggression, with surrogate forces, covert support, cyber-attacks, people in green without military insignia, in addition to propaganda campaigns and economic, political pressures, as well as open military pressure at the border, for sending the message. And even invoke the threat with the nuclear option. The problem is what we must do to make the deterrent effective not only against the 20,000 soldiers who threaten to cross the border, but also for situations like the one described in Ukraine, which we saw in Georgia, in Transnistria. We are working on this now, in counteracting the hybrid type war, in contingency plans, in the political lines that we will update, and these things will determine what kind of political, military, civilian capabilities NATO must have in order to have a deterrent effective against this kind of war*”[1].

NATO's concept of countering hybrid actions

Generally, the efforts that both NATO and the EU, as well as the individual member states, undertake are geared towards the evolution of the Armed Forces (AF) in terms of training and materiel in order to successfully execute actions, operations or campaigns specific to the new type of conflict, but also to the society as a whole, in order to increase the resilience of the population and institutions in the face of hybrid threats.

Since its establishment and until now, the North Atlantic Alliance has made constant efforts to update its strategic concept in line with the new types of risks that threatened the security and safety of the Member States. If, during the Cold War, the enemy was known (USSR / Warsaw Pact) and the threats were relatively easy to identify and combat, the emergence of the hybrid conflict raises a new concern among NATO (and EU) members for successfully counteracting it.

Inside NATO, *the approach to the field of hybrid threats* has two stages, the first being generated by the emergence in the US military society of hybrid war theories, and the second triggered by the ongoing crisis in Ukraine.[2]

Thus, in a first phase, the debates in the American military academic environment on the topic of hybrid warfare gave birth in 2010, at the Allied Command for Transformation (ACT), of a document in which the concept is defined very generally: “*Hybrid threats are generated by adversaries who have the ability to use both conventional and unconventional means simultaneously to achieve their goals*”[3]. In addition, it was appreciated that the combination of non-military means (political, economic, and diplomatic) with military ones generates difficulties for NATO which, as a political-military organization, must unload most of the actions to counter hybrid threats to the area of authorities and civil societies in Member States.

The year 2014 constituted the transition to a new phase in the evolution of the organization, when NATO returned to the mission for whom it was set up - collective defence – with the emergence of the crisis in Ukraine and the way of manifesting the hybrid threats. But the inability to identify the aggressor as a particularity of the contemporary hybrid

[1] Luca A. Popescu, *US official on Russia's threat to Europe: "he is such a reckless adversary that he collides with a NATO military force?”,* article published by the online news agency Mediafax, https://www.mediafax.ro/externe/oficial-nato-despre-rusia-e-adversarul-atat-de-nesabuit-incat-sa-se-ciocneasca-cu-o-forta-nato-13063080 accesed 04.03.2019.

[2] Teodor Frunzeti, Marinel-Adi Mustață, Cristian Toader, Cristian Bărbulescu, *Increased resilience to hybrid threats through good governance,* Report related to the research project, The Academy of Romanian Scientists, pp.27-29,http://www.aosr.ro/wp-content/uploads/2018/02/Raport-Proiect-AOSR_final-1.pdf accesed18.02.2019.

[3] *** *Bi-SC input to New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats*, NATO, August 25, 2010, p. 2, https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf accesed 24.02.2020.

conflict makes the activation of art. 5 of the Washington Treaty (the act establishing NATO) more difficult and less certain, this solidarity clause being conceived against conventional and traditional military threats when the treaty was signed.

In NATO's vision, the main sectors of action for increasing the resilience of the Allied nations are critical infrastructure and civil society.[4] To this end, Member States are urged to take all necessary measures to ensure the continuity of management and safety of critical infrastructure systems (transport, energy, communications, finance, etc.), the preparation of the population for action in crisis situations, and the maintenance of logistics lines for AF if they are to be deployed.

Moving from theory to practice, counteracting hybrid warfare has come to NATO's attention since July 2009, when the International General Staff (IMS) requested the Alliance's strategic commands, Supreme Allied Commander (SAC) and ACT, several points of view to develop a fundamental concept regarding the military contribution in order to counteract these types of threats.

The following year, on 25 August 2010, SAC and ACT submitted to the Member States a project entitled *Military Contribution to Countering Hybrid Threats*[5], which was not approved by the North Atlantic Council (NAC) and was frozen until 2014. Following the annexation of the Crimean Peninsula by the Russian Federation and the outbreak of the crisis in South-Eastern Ukraine, discussions on the topic of hybrid warfare resumed, with emphasis on threat assessment, identification and evaluation of response measures, as well as on the capabilities needed to counteract the military aspects of hybrid threats, while simultaneously preparing forces and means especially designed to respond to such threats.[6]

In the opinion of the NATO Secretary General (SG) of that period, Anders Fogh Rasmussen, the Alliance did not have at its disposal the most suitable methods and means of counteracting hybrid threats. NATO SG appreciated that the response to a possible hybrid conflict against the Alliance does not fall within the normal competences of the Allied commandments, which are prepared to carry out mainly military operations, not actions in the sphere of economic and social life, such as those in the economic (prohibition of access to advanced resources and technologies, economic sanctions, etc.) or informational sectors (cyber attacks in order to block the activity of public institutions or to interrupt the supply of drinking water and electricity, propaganda, manipulation or different types of attacks information specific to the social-media domain, etc.).[7]

This variety of features and manifestations of the hybrid conflict forced the North Atlantic Alliance to make sustained efforts to defend its members. From this perspective, some actions, such as the transformation of the AF, the flexibility of the combat units and the increase in mobility (for force projection and rapid reaction), including the prepositioning of advance elements (with small troops and technical deposits, ammunition and other military materials), are necessary but not enough. In order to complete the set of measures to counter hybrid threats, it is necessary for NATO to identify those measures which, when applied in an integrated manner by Member States at Alliance level, will either minimize the use of armed forces in some cases or multiply their effects in other situations.

[4] *** *Commitment to enhance resilience*, Commitment to strengthen the resilience assumed by the allied states at the NATO Summit in Warsaw (July 6-8, 2016), https://www.nato.int/cps/en/natohq/official_texts_133180.htm accesed 24.02.2020.

[5] *** *Bi-SC input to New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats*.

[6] Peter Pindják, *Deterring hybrid warfare: a chance for NATO and the EU to work together?*, in NATO Magazine, November 18, 2014, https://www.nato.int/docu/review/articles/2014/11/18/deterring-hybrid-warfare-a-chance-for-nato-and-the-eu-to-work-together/index.html accesed 24.02.2020.

[7] Viorel Buţa, Valentin Vasile, *Perspectives on the evolution and influence of the concept of hybrid warfare (II),* in the Romanian Military Thought magazine no.4, October-December 2015, The Romanian General Staff publishing house, Bucharest, 2015, p. 20.

At present, like other Romanian authors[8], we consider that informational attacks are one of the main threats of hybrid type to the security state of NATO member states. The complexity of these threats has caused major concerns at Alliance level, which were addressed in a framework document that envisaged the future security environment in the perspective of the 2030s and presents the strategic military principles: operational agility, security networking, shared resilience, strategic awareness and strategic communication (StratCom).[9] As we can see, the vast majority of the actions that these strategic directions involve are based on the informational environment, from the security of the information networks to the strategic communication.

From NATO's point of view, ensuring the security of computer networks requires a proactive attitude not only from the Member States, but also from the Alliance's partners, in order to be able to anticipate, overcome and neutralize hybrid threats. In addition to the ability to model the informational environment through a continuous interaction, both physical or virtual, we should increase the importance and weight of the information operations in the actions of counteracting the hybrid actions, in order to attract as many partners as possible to their own strategic goals and thus achieving the proposed tactical and operational objectives.

Another important concept for the Alliance that is closely correlated with the informational domain is the strategic communication (StratCom), which represents the coordinated use of diplomatic, public relations, informational operations (InfoOps) and psychological operations (PSYOPS), coordinated at all levels and synchronized with military actions, in order to achieve the Alliance's goals and objectives.

Currently, InfoOps can be included in the unconventional pattern of hybrid aggressions due to the nonviolent features they impose. Although they belong exclusively to the military field, InfoOps are of particular importance in modern hybrid conflicts, though they have their origins during the Cold War. After the Second World War, the conflict between the two big blocs, NATO and the Warsaw Pact, not only meant a confrontation between the military potentials of the two politico-military organizations, but also a collision of the systems of social organization, communism and capitalism. This confrontation of ideologies gave birth to new concepts, such as ideological or ideas warfare, political communication, psychological operations, etc., which created confusion because they used *weapons* that were not truly distinct, all belonging to a single domain - media (radio, TV, press). After the end of the Cold War, an explosion of the level of access of the population to the public means of information took place, which will be at the basis of the importance of the InfoOps role in the confrontation between East and West. However, it is surprising, given the widespread public access to the media (especially the so-called social media), how successful Russia's misinformation actions have been in Ukraine, but also internationally, including Europe and the US.

Shortly after the annexation of the Crimean Peninsula and the start, in our opinion, of a frozen conflict in South-Eastern Ukraine, the North Atlantic Alliance is forced to take concrete steps towards countering hybrid threats. Thus, in the statement of the NATO Summit in Wales, several directions of action are presented for the preparation of the Member States in order to counteract the hybrid threats, on the command line, education and training, communications, military intelligence (INTELL), interoperability, protection, weapons of mass destruction (WMD) and network systems.

[8] Cristian, Petre, *Information component - essential element of military operations in the third millennium*, in the Romanian Military Thought magazine no.1, January-March 2016, The Romanian General Staff publishing house, Bucharest, 2016, pp.172-173.

[9] *** *MCM-0199 2015 – Framework for Future Alliance Operations*, Supreme Allied Commander Transformation, Enclosure 1 to MCM-0199-2015, https://www.act.nato.int/images/stories/media/doclibrary/ffao-2015.pdf accesed 24.02.2020.

In general, *NATO's mode of action* is based on four strategic directions, *construction, deterrence*, *employment and stabilization* which, although interdependent, are not always strictly applicable in a predetermined order and can be used simultaneously or even partially. It is precisely this relative independence which can successfully counteract hybrid aggression, of course by applying the specific methods and means of the hybrid domain and considering their main characteristics.

Also, in order to successfully counteract hybrid aggression, NATO intends to create a set of complementary methods and actions, covering all fields of activity, political, diplomatic, economic, social, informational, military, etc., while identifying means and directions of action to achieve this goal, which is, in itself, a time-consuming process.

At the same time, the Alliance must make efforts to raise awareness among Member States and allies or partners of the obligation to respond firmly to any type of aggression against the safety and security of nations, whether conventional or hybrid, and this obligation requires these states to engage long term because security can only be maintained through consultations, deterrence, defence, crisis management and partnerships with law enforcement agencies, local authorities and other relevant actors in this context.

The EU approach to counteracting hybrid actions

With NATO's hybrid efforts as its basis and an example worth emulating, the EU also took the necessary steps to define, identify and counteract hybrid threats immediately after the crisis in Ukraine. Thus, in July 2014, the President of the European Commission, Jean-Claude Juncker, declared that the member states of the Union are now required to better coordinate their national policies so that "*Europe will be stronger in terms of security and defence*"[10].

The first initiative in this domain belongs to the European Commission, which, on 28 April 2015, adopted the *European Security Agenda*, a programmatic document outlining the main directions of action of the Union in the period 2015-2020 for: improving the exchange of information; the prevention of radicalization; combating terrorism, organized crime and cyber crime; protecting citizens and critical infrastructures. The Agenda also warned that „threats such as those posed by cyber terrorism and hybrids may intensify in the coming years"[11].

Subsequently, on May 18, 2015, the Foreign Affairs Council (FAC) called on the EU to develop a *Joint Framework for Counteracting Hybrid Threats*, which would contribute to increasing the resilience of EU member states and partners. One year later, Federica Mogherini, the EU High Representative for Foreign Affairs and Security Policy, together with the European Commission, proposed (April 6, 2016) the *Joint Framework on Countering Hybrid Threats - A European Union Response*[12] which, as the title also shows, describes the hybrid threats and outlines the main ways of counteracting them from a European perspective, as follows:

- *"The concept* (A/N hybrid threat) *aims to encompass the mix of coercive and subversive activities, conventional and unconventional methods, which can be used in a coordinated manner by state or non-state actors to achieve specific goals, but still below the state threshold of officially declared war. Usually, the focus is on exploiting the vulnerabilities of the target and on generating ambiguity in order to prevent decision-making*

[10] Jean-Claude Juncker, *Let's get Europe moving*, speech in the European Parliament, July 15, 2014, Strasbourg, https://ec.europa.eu/commission/sites/beta-political/files/juncker-political-guidelines-speech_ro.pdf accesed 14.06.2019.

[11] *** *Commission takes steps to strengthen EU cooperation in the fight against terrorism, organised crime and cybercrime*, The European Agenda on Security, The European Commission, Strasbourg, April 28, 2015, p. 13, https://ec.europa.eu/commission/presscorner/detail/en/IP_15_4865 accesed 24.02.2020.

[12] *** *Joint framework for countering hybrid threats - A response from the European Union,* Brussels, 6.4.2016 JOIN(2016) 18 final.

processes. Massive misinformation campaigns, which use social media platforms to control political discourse or to radicalize, recruit and coordinate intermediary actors can be vectors of hybrid threats"[13];

- EU member states have their own responsibility for countering hybrid threats, because each presents specific vulnerabilities, while the EU supports this process only for common threats, such as those that manifest across borders (eg immigration, organized crime, drug trafficking, persons, weapons, hazardous materials, etc.);
- The European vision for countering hybrid threats is based on existing sectoral strategies (such as the EU Global Strategy, the Cyber Security Strategy, the Energy Security Strategy, the Maritime Security Strategy);
- In order to counteract hybrid threats, cooperation between the EU and NATO is needed.

EU responses to counteracting hybrid aggression include proposals for action by Member States, but also valid at Union level, such as: recognizing the hybrid threat and empowering Member States to identify their own vulnerabilities and their specific indicators; increasing the level of resilience of governmental institutions and national societies as a whole; improving the crisis management system, with emphasis on prevention, response and return to the status quo ante; last but not least, the development of collaboration and coordination relations with NATO, in particular regarding early warning and strategic situation awareness, strategic communication, cyber security and crisis prevention and management.

From the perspective of some Romanian authors[14], the notion of hybrid has an added connotation in the European approach by integrating a series of different threats that do not automatically have a connection with each other (such as terrorism, cyber attacks and the conventional threat represented by Russia), but they produce effects throughout the European territory. For this reason, two types of hybrid threats are identified in the European literature: one in which the actions are led by a state actor and the second in whom they belong to a non-state entity. The novelty of the European approach, however, is how to counteract the aggressions associated with the hybrid war, respectively by resilience to hybrid threats.

Considering the need to counter threats and the request of the FAC to the EU on the elaboration of the Joint Framework for Countering Hybrid Threats, the European Council adopted, on 28 June 2016, the *EU's Global Strategy on Foreign and Security Policy*, in which hybrid threats are considered the main risks to the Union, along with terrorism, organized crime, cyber attacks, economic volatility, climate change and energy insecurity (but even these can be considered at particular points in time to belong to the hybrid domain if used properly by an innovative aggressor). Also identified are the main areas of action: strengthening the security of the member states, increasing the resilience of the states in the Eastern and Southern vicinity of the EU, the integrated approach to conflicts, the dimensions of regional cooperation and the rules of behavior for ensuring peace and security, prosperity and democracy at the international level.[15]

To apply the stipulations of the Global Strategy, the EU High Representative for Foreign Affairs and Security Policy, F. Mogherini, submitted (14 November 2016) a plan to the Council of the European Union, entitled the *Security and Defence Implementation Plan*, which complements the series of EU documents on security and defence of the Member States and stresses the importance of strengthening countries' defence and response capacities

[13] *Ibidem*, p. 2.

[14] T. Frunzeti, M.A. Mustață, C. Toader, C. Bărbulescu, *op.cit*, pp. 24-27.

[15] V. Buța, V. Vasile, *Counteracting hybrid threats from the perspective of the European Union*, in the Romanian Military Thought magazine no.1, January-March 2017, The Romanian General Staff publishing house, Bucharest, 2017, pp. 51-53, 57-58.

in the event of conflict or external crisis, including combating hybrid aggression, while proposing further directions for action. It is worth noting the mention in the Plan according to which "*civilian or military experts can make a significant contribution to increasing the EU's capacity for analysis and interaction in a state where there is a risk of violence, instability or hybrid threats*"[16].

Also, the European institutions adopted the *EU Operational Protocol for Counteracting Hybrid Threats* (EU Council, 14 November 2016), the *European Defence Action Plan* (European Commission, 30 November 2016), as well as various EU sectoral strategies, including the *EU Cyber Security Strategy* (published in February 2013 and completed in December 2015 with the Directive on Network and Information Security), the *Strategy on Maritime Security* (2014) or the *Strategy for Energy Security* (2014).

The *EU Operational Protocol for Counteracting Hybrid Threats* has been drafted on the basis of requests submitted by the *Joint Framework for Countering Hybrid Threats* to the European Commission and the High Representative for Foreign Affairs and Security Policy, the two EU institutions being induced, in cooperation with the Member States, to develop "*a joint operational protocol for conducting periodic exercises to improve the strategic decision-making capacity, in response to complex hybrid threats based on crisis management procedures and EU integrated crisis response mechanisms*"[17]. In fact, the Operational Protocol contains "*effective procedures that can be followed in the case of hybrid threats, from the initial phase of identification to the final phase of the attack, and which specify the role of each institution and each EU actor during this process*"[18]. Through these procedures, an EU-level institutional coordination in INTELL domain is described, the necessary capabilities are inventoried, and the political directives and decision-making process in the case of hybrid aggression against Member States and partners are presented. Likewise, the levels of coordination (political-strategic, operational and technical) for the management of actions in the hybrid field and the training needs of the EU and the Armed Forces of the Member States are specified. Furthermore, the Protocol capitalizes on and develops existing mechanisms at EU level for crisis management and cooperation with partner organizations, primarily with NATO.

As a highlight of the EU's efforts in the hybrid sphere, on 21 November 2016, the Undersecretary of State and Deputy Director General in the Department of European Affairs of the Government of Finland, Jori Arvonen, announced the initiation of the procedures for setting up in the capital of Finland, Helsinki, a *Center of Excellence* (CoE) *of the EU for combating hybrid actions*. According to the Finnish official, the initiative to set up this CoE was supported by NATO and the US, aimed at "*strengthening the resilience of the parties involved and preparing them to deal with hybrid threats through training, applied research and the exchange of good practices*"[19]. With its inauguration (3 October 2017), the CoE from Finland joins other initiatives taken at European level (eg StratCom Working Group of the European External Action Service) and Euro-Atlantic (NATO CoE from Latvia in the StratCom domain), complementary to the hybrid domain. On 14 November 2018, **Romania** signed the participation memorandum and thus becomes the 19th Member State, together with Austria, Canada, Czech Republic, Denmark, Estonia, Finland, France, Germany, Italy, Latvia, Lithuania, Norway, Poland, Spain, Sweden, Netherlands, UK and USA.

[16] *Ibidem,* p.11.

[17] *** *Joint Framework on Countering Hybrid Threats,* Action 19, The European Commission, JOIN(2016) 18 final, Brussels, April 7, 2016, p.17, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 accesed 24.02.2020.

[18] *** *Joint Staff Working Document: EU Operational Protocol for Countering Hybrid Threats – EU Playbook*, Council of the EU, SWD(2016) 227 final, Brussels, July 7, 2016, p. 2.

[19] Jussi Rosendahl, *Finland Plans to Set up Center to Counter 'Hybrid' Threats*, Reuters World News, November 21, 2016.

NATO-EU partnership to counter hybrid actions

To successfully counteract hybrid aggression, the EU works with regional or international organizations, such as the Organization for Security and Cooperation in Europe (OSCE) and the United Nations (UN), but its special military partner is the North Atlantic Alliance. The EU and NATO cooperate in many areas to identify and counteract hybrid threats, such as strategic situation awareness, STRATCOM, security of cyber space, crisis prevention and response, with a formal and informal dialogue, constantly synchronizing the efforts of the two entities.

On 16 December 2002, the first formalization of EU-NATO collaborative relations took place, with the adoption of a joint declaration by which the two organizations have opted for a strategic cooperation type of partnership, political consultations and mutual support for crisis management and conflict prevention, with NATO to support EU operations or campaigns with information and planning capabilities or military resources.

A few months later, the Berlin+ agreement was signed (March 1, 2003), which represents a continuation of the Berlin Summit in 1996, when NATO-EU cooperation was first discussed. This new Berlin+ agreement was needed to provide for the ways in which NATO can indirectly support crisis management at EU level with resources and capabilities for operational planning and command-control (C2).

Until the crisis in Ukraine broke out (2014), although several initiatives were taken at EU level to implement a Common Defence and Security Policy, no significant actions were taken in the Union's partnership with the North Atlantic Alliance. After the occupation of the Crimean Peninsula by Russia and the outbreak of fighting in Donbass (the Donetsk and Lugansk regions of South-Eastern Ukraine) between pro-Russian separatists and Ukrainian forces, the NATO SG, A.F. Rasmussen appreciated (August 2014) that „*more than NATO will be needed to effectively counter such a hybrid war*”[20].

Considering the number of actions carried out by both the EU and NATO before the Ukrainian crisis, compared to the activities following the annexation of the Crimean Peninsula, we can see that 2014 is the crossroads point in the hybrid threat research for both organizations.

Thus, starting with the NATO Summit in Wales (September 2014), NATO began to pay much more attention to the hybrid domain. By the statement adopted at the NAC meeting on September 6, 2014, the leaders of the Allied countries wanted to ensure that *“**NATO is able to effectively address the specific challenges of hybrid warfare threats**, which involve the use of a wide range of open, military, paramilitary and civilian measures undercover, in architecture with a high degree of integration. It is essential that the **Alliance has the tools and procedures necessary to effectively deter and respond to the threats of hybrid warfare**, as well as the capabilities to strengthen national forces. **This also includes** the development of strategic communications, the development of hybrid warfare exercise scenarios and the **strengthening of coordination between NATO and other organizations**, according to relevant decisions taken, in order to improve information exchange, political consultation process and internal coordination”*[21].

At the same time, the leaders of the NATO countries *“express their interest in **continuing the dialogue and cooperation between NATO and the EU**. Our consultations*

[20] Ian Traynor, *Ukraine crisis: NATO plans East European bases to counter Russia (NATO chief announces move in response to Ukraine crisis And says Alliance is dealing with a new Russian military approach)*, article in The Guardian, August 27, 2014, https://www.theguardian.com/world/2014/aug/26/nato-east-european-bases-counter-russian-threat accesed 24.02.2020.

[21] *** *Statement of the NATO Summit in Wales*, adopted by the Heads of State and Government attending the North Atlantic Council meeting in Wales, September 4-5 2014, art.13, https://www.mae.ro/sites/default/files/file/2014/pdf/2014.09.06_declaratie_summit.pdf accesed 21.02.2020.

have expanded to cover issues of concern to both organizations, including security challenges such as cyber defence, proliferation of WMD, counter-terrorism and energy security. We will also seek to work more closely in a number of other areas, including maritime security, capacity building in the field of defence and security, and ***to address hybrid threats*** *in accordance with the decisions taken"*[22].

Beginning with 2016, the EU also started to focus more on working with NATO to successfully combat hybrid aggression. In this regard, the *Joint Framework on Countering Hybrid Threats - A European Union response* attaches particular importance to cooperation with NATO in identifying the most appropriate action options for counteracting hybrid aggression. From the perspective of this document, the two organizations are asked to work together to fulfill the common purpose represented by unconventional, asymmetrical or hybrid threats against the Member States.

A few months away, the European Union's Global Strategy on Foreign and Security Policy aims to "*deepen the partnership with NATO by coordinated development of defence capabilities, exercises in parallel and synchronized, mutual support actions to strengthen the capabilities of our partners, countering hybrids threats and cyber security, as well as promoting maritime security*"[23]. In addition, the EU intends that this Global Strategy establishes the level of political-military ambition and the directions of capacity development that the Member States will dislocate under European mandate for carrying out missions, independently or in cooperation with NATO.

On the other hand, the declaration adopted at the ending of the 2016 NATO Summit in Warsaw (July 8-9) announced the Alliance's long-term plans for "*a strategy on the role of NATO in countering the hybrid war, which will be implemented in coordination with the European Union*"[24]. At the same time, the participants in the summit agreed to support the establishment of the EU CoE for combating hybrid actions, which **Romania** would eventually join in 2018.

The Warsaw Summit also saw a NATO-EU Joint Declaration, which was signed by the EU Council President Donald Tusk and the European Commission President, J.C. Juncker, and from NATO by the SG of Alliance, Jens Stoltenberg. Through this statement, the two organizations highlighted the level of cooperation and the results obtained during the almost 15 years since the establishment of the strategic partnership, and for the future emphasize the need for measures to "*increase the common capacity to counter hybrid threats, including strengthening resilience and development of the cooperation for the analysis, prevention and early identification (of threats), timely mutual information and carrying out, at the possible level, the exchange of intelligence, coordination of strategic communication and response measures*"[25].

At European level, the EU Council adopted (14 November 2016) the *Implementation Plan on Security and Defence*, in which F. Mogherini, leading the European External Action Service at the time, emphasized thr mutual defence and solidarity clauses provided for in the Treaty on European Union (TEU), at art. 42, paragraph (7), and the Treaty on the Functioning of the European Union (TFEU), at art.222. The plan states that "***NATO remains the***

[22] *Ibidem*, art.104.

[23] *** *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, European Council, Brussels, June 2016, p. 37, https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf accesed 24.02.2020.

[24] *** *NATO Warsaw Summit Communiqué*, adoptat de şefii de stat şi de guvern participanţi la summit-ul NATO de la Varşovia, 8-9 iulie 2016, art. 37, lit. i, https://www.nato.int/cps/en/natohq/official_texts_133169.htm accesed 24.02.2020 art.37, lit.i.

[25] *** *Joint Declaration*, Joint statement by the President of the European Council, the President of the European Commission and the Secretary General of NATO, Warsaw, July 8, 2016.

foundation for the collective defence for those States which are members of it”[26], specifying that the seven areas of cooperation with the Alliance provided for in the NATO - EU Joint Declaration adopted at the NATO summit are maintained by developments during the Warsaw Summit, respectively: counteracting hybrid threats; operational cooperation, including maritime and related to the migration of persons; cyber security and defence; developing defence capabilities; military industry and scientific research; exercise planning; and supporting partners in Eastern and Southern Europe to develop security and defence capabilities.

Just a week away (23 November 2016), the European Parliament adopted the *Resolution on the Implementation of the Common Security and Defence Policy*, welcoming the NATO - EU Joint Declaration of Warsaw, but at the same time appreciated that it „*describes informal practices [which are] well established, rather than bringing EU - NATO cooperation to a new level*”, stressing “***the need to deepen cooperation*** *and further complete the generation of capabilities corresponding to hybrid and cyber threats...*”[27]. Due to rather negative appraisals, the European Parliament resolution emphasized that EU security, often perceived as deeply interconnected, is rather interdependent and vulnerable because Member States “*react to common threats and risks in an uncoordinated and fragmented way, which complicates and often even hinders their unitary approach*”, considering that the EU “*does not have the resilience to effectively counter hybrid threats, which often have a cross-border dimension*”[28].

Conclusions

Countering the threats specific to any type of war (conventional, asymmetrical, hybrid, etc.) requires different capabilities related to all areas of human life (political, military, diplomatic, economic, social, informational, etc.), as well as capitalization on the power potential they offer, but in accordance with the pattern of conflict. In this way, the main EU programmatic documents in the field of the Common Security and Defence Policy (CSDP) must be interpreted - the *European Security Agenda*, the *European Union's Global Strategy on Foreign and Security Policy* and the *sectoral strategies* on cyber, energy and maritime security.

The study of hybrid threats, which characterize modern confrontations, and the need to counteract them, has led to the need to supplement EU sectoral strategies with other documents that scientifically argue and justify / legitimize the ways and directions of action to combat hybrid aggression, characterized by the combined use of methods and the traditional / conventional means with the unconventional ones (asymmetrical / hybrid). Thus, the *Joint Framework for Countering Hybrid Threats*, the *EU Operational Protocol for Countering Hybrid Threats*, the *Security and Defence Implementation Plan* and the *European Defence Action Plan* appear.

At Euro-Atlantic level, we appreciate that, as a predominantly military alliance, NATO does not have the possibility to cover the full range of hybrid threats, especially those that do not involve the use of violence or those that involve the use of violence, but are within the competence of law enforcement. Still, we acknowledge that it has taken concrete and important steps in the development of plans and strategies or in the creation and development

[26] *** *Implementation Plan on Security and Defence,* High Representative of the Union for Foreign Affairs and Security Policy, Vice-President of the European Commission, and Head of the European Defence Agency, EU Council, Brussels, November 14, 2016, p. 4, https://www.consilium.europa.eu/media/22460/eugs-implementation-plan-st14392en16.pdf accesed 24.02.2020.

[27] *** *European Parliament Resolution on the Implementation of the Common Security and Defence Policy*, based on the Council's Annual Report to the European Parliament on the Common Foreign and Security Policy, 2016/2067(INI), Strasbourg, November 23, 2016, pct. 36.

[28] *Ibidem.*

of specialized structures to combat unconventional risks and threats (such as counter-terrorism and cyber defence). For this reason, it is necessary to deepen NATO's partnership with other international organizations, but especially with the EU, due to the large number of states belonging to both organizations, 21 of the 27 member states of the Union and 29 respectively in the case of the North Atlantic Alliance.

All political or military-political organizations are based on a mutual assistance clause, whether it is called a collective defence clause in NATO or a mutual defence clause in the EU, so that an attack on a Member State will automatically trigger everyone's reaction, being obliged by the treaty to establish the alliance / union to intervene in the support of the aggressed state. The stipulations of this principle, also known as the motto "*All for one, one for all!",* are generally similar regardless of organization, at EU level being stipulated in Art. 42 paragraph (7) of the TEU, in the case of NATO in art. 5 of the North Atlantic Treaty, being recognized including by the Charter of the United Nations, at art. 51. Going back to the dual membership status of many European states, both EU and NATO, we can see that the two organizations are almost doubling their system of mutual security guarantees that the Member States benefit from.

But, in the case of hybrid threats, it is particularly difficult if not impossible to identify the attacker, whether it is a state or a non-state entity, which is one of the characteristics of hybridity. In these circumstances, more than likely, the potential aggressor denies the interference and the paternity of the attack, which will lead to the impossibility of reaching the necessary consensus regarding the definition of aggression as an armed attack against a Member State. From this perspective, the invocation of the TEU mutual defence clause or the principle of collective defence in the North Atlantic Treaty will depend on the possibility of identifying the aggressor and classifying his actions in the category of armed attack against a Member State.

So, in order to identify and counteract hybrid actions, there is a need for a set of means and methods that the Alliance cannot have due to the limitations generated by the role and missions that were the basis of its establishment, the best solution being the cooperation with EU. This issue is in the attention of the two organizations, between which there is already a very good cooperation in the field of cyber defence, but that can be extended to other areas specific to hybrid threats, because the EU has a wide range of tools that can be used to combat the most specific components of this type of conflict. Given that there are 21 states with dual membership of the EU and NATO, the Union is the most appropriate solution to increase the Alliance's capabilities in the hybrid domain, the two organizations being able to offer a wide and comprehensive range of military and non-military resources (diplomatic, political and economic) to counteract hybrid threats. The NATO - EU strategic partnership is already recognized by the 2014 NATO Summit (Wales) final statement, and the hybrid threats to the Euro-Atlantic states will lead to its development.

But at the same time, the potential of the EU and NATO partner states, especially those located in the buffer zones between one of the two organizations, NATO or the EU, with the Russian Federation or other problematic states (Iran, Korean DPRK) must not be forgotten, and neither those which have a pro-Western orientation, as is the case of Georgia, Moldova and even Ukraine.

BIBLIOGRAPHY

1. BUŢA, Viorel; VASILE, Valentin, *Perspectives on the evolution and influence of the concept of hybrid warfare (II)*, in the Romanian Military Thought magazine no.4, October-December 2015, The Romanian General Staff publishing house, Bucharest, 2015;

2. BUȚA, Viorel; VASILE, Valentin, *Counteracting hybrid threats from the perspective of the European Union*, in the Romanian Military Thought magazine no.1, January-March 2017, The Romanian General Staff publishing house, Bucharest, 2017;
3. CULLEN, Patrick J.; Erich REICHBORN-KJENNERUD, *What is hybrid warfare?*, Norwegian Institute for International Affairs, Policy Brief 1/16, 2016; THIELLE, Ralph D., *The New Colour of War – Hybrid Warfare and Partnerships*, ISPSW Strategy Series: Focus on Defence and International Security, Issue No.383, October 2015;
4. FRUNZETI, Teodor; MUSTAȚĂ, Marinel-Adi; TOADER, Cristian; BĂRBULESCU, Cristian, *Increased resilience to hybrid threats through good governance*, Report related to the research project, The Academy of Romanian Scientists, http://www.aosr.ro/wp-content/uploads/2018/02/Raport-Proiect-AOSR_final-1.pdf
5. JUNCKER, Jean-Claude, *Let's get Europe moving*, speech in the European Parliament, Strasbourg, July 15, 2014, https://ec.europa.eu/commission/sites/beta-political/files/juncker-political-guidelines-speech_ro.pdf.
6. PETRE, Cristian, *Information component - essential element of military operations in the third millennium*, in the Romanian Military Thought magazine no.1, January-March 2016, The Romanian General Staff publishing house, Bucharest, 2016;
7. PINDJÁK, Peter, *Deterring hybrid warfare: a chance for NATO and the EU to work together?* in NATO Magazine, November 18, 2014, https://www.nato.int/docu/review/articles/2014/11/18/deterring-hybrid-warfare-a-chance-for-nato-and-the-eu-to-work-together/index.html
8. POPESCU, Luca A., *US official on Russia's threat to Europe: „he is such a reckless adversary that he collides with a NATO military force?"* article published by the online news agency Mediafax, https://www.mediafax.ro/externe/oficial-nato-despre-rusia-e-adversarul-atat-de-nesabuit-incat-sa-se-ciocneasca-cu-o-forta-nato-13063080
9. ROSENDAHL, Jussi, *Finland Plans to Set up Center to Counter 'Hybrid' Threats*, Reuters World News, November 21, 2016;
10. TOADER, Vasile; RICU, Adrian, *Hybrid warfare - an interinstitutional approach*, in the Romanian Military Thought magazine no.1, January-March 2016, The Romanian General Staff publishing house, Bucharest, 2016;
11. TRAYNOR, Ian, *Ukraine crisis: NATO plans East European bases to counter Russia (NATO chief announces move in response to Ukraine crisis and says Alliance is dealing with a new Russian military approach)*, article in The Guardian, August 27, 2014, https://www.theguardian.com/world/2014/aug/26/nato-east-european-bases-counter-russian-threat
12. *** *Bi-SC input to New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats*, NATO, August 25, 2010, https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf
13. *** *Commission takes steps to strengthen EU cooperation in the fight against terrorism, organised crime and cybercrime*, The European Agenda on Security, The European Commission, Strasbourg, April 28, 2015;
14. *** *Commitment to enhance resilience*, Commitment to strengthen the resilience assumed by the allied states at the NATO Summit in Warsaw (July 6-8, 2016), https://www.nato.int/cps/en/natohq/official_texts_133180.htm
15. *** *Common framework for countering hybrid threats - A response from the European Union*, Brussels, 6.4.2016 JOIN (2016) 18 final;
16. *** *Statement of the NATO Summit in Wales*, adopted by the Heads of State and Government attending the North Atlantic Council meeting in Wales, September 4-5,

2014, https://www.mae.ro/sites/default/files/file/2014/pdf/2014.09.06_declaratie_summit.pdf

17. *** *European Parliament Resolution on the Implementation of the Common Security and Defence Policy* based on the Council's Annual Report to the European Parliament on the Common Foreign and Security Policy, 2016/2067(INI), Strasbourg, November 23, 2016;
18. *** *Joint Framework on Countering Hybrid Threats,* Action 19, The European Commission, JOIN(2016) 18 final, Brussels, April 7, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018
19. *** *Joint Staff Working Document: EU Operational Protocol for Countering Hybrid Threats – EU Playbook*, Council of the EU, SWD (2016) 227 final, Brussels, July 7, 2016;
20. *** *Joint Declaration,* Joint statement by the President of the European Council, the President of the European Commission and the Secretary General of NATO, Warsaw, July 8, 2016;
21. *** *Implementation Plan on Security and Defence*, High Representative of the Union for Foreign Affairs and Security Policy, Vice-President of the European Commission, and Head of the European Defence Agency, EU Council, Brussels, November 14, 2016, https://www.consilium.europa.eu/media/22460/eugs-implementation-plan-st14392en16.pdf
22. *** *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy,* European Council, Brussels, June 2016, https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf
23. *** *MCM-0199 2015 – Framework for Future Alliance Operations*, Supreme Allied Commander Transformation, Enclosure 1 to MCM-0199-2015, https://www.act.nato.int/images/stories/media/doclibrary/ffao-2015.pdf
24. *** *NATO Warsaw Summit Communiqué*, adopted by heads of state and government participating in the NATO summit in Warsaw, July 8-9, 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm

THE HYBRID WAR IN THE EAST-WEST PARADIGM

Viorel BARBU
Colonel, Ph.D. Candidate, Ministry of National Defence, Bucharest, Romania
viorel_barbu_map@yahoo.com

Abstract: *The popularization of the concept of hybrid conflict begins with the aggression of the Russian Federation against Ukraine, resulting in the illegal annexation of the Crimean Peninsula and the conflict with freezing tendencies in South-Eastern Ukraine. Thus, starting in 2014, states have begun to review their security policies and strategies, succeeding in defining their vulnerabilities, risks and threats of hybrid type and, to a lesser degree (and with few exceptions), adapting their doctrines and institutions to the new reality. To date, few states have achieved a developed level of hybrid capabilities. Apart from "the big three", the USA, the Russian Federation and the People's Republic of China, other states, political-military organizations and even non-state actors have begun to take important steps in the field. The states with important doctrines and capabilities, we mention the United Kingdom, Germany, France, Italy and Israel, and at the level of organizations, only the Western ones, NATO and the EU, have policies and means of enforcement that cover to a certain extent the spectrum of unconventional aggression. Non-state entities, such as the terrorist organizations Al-Qaeda and ISIL, which have only asymmetrical capabilities, some of which are significant, should not be overlooked. If Russia has already begun to implement hybrid strategies, doctrines and tactics, we naturally ask ourselves why the West seems to have lagged behind in this area and what it could do to reduce the distance between it and Russia in coping with this type of aggression.*

Keywords*: unconventional threats, asymmetric, hybrid warfare, terrorism, security policies and strategies*.

Introduction

The popularization of the concept of hybrid conflict starts with the aggression of the Russian Federation against Ukraine, resulting in the annexation of the Crimean Peninsula and the start of the secession war in the Donetsk and Lugansk provinces of South-Eastern Ukraine (Donbass region). Thus, the majority of states started, in 2014, to review their security policies and strategies, in an attempt to define their hybrid risks, vulnerabilities and threats, as well as adapting doctrines and institutions to the new geopolitical reality.

Currently, at most 10 nations have achieved hybrid capabilities. Apart from the "*big three*" who have unconventional capabilities - the US, Russian Federation and People's Republic of China - only some states, organizations or other actors have started to take important steps in this field. Of these, the UK, Germany, France, Italy and Israel have important hybrid doctrines and capabilities, while some non-state entities, such as the terrorist organizations Al Qaeda and the Islamic State of Iraq and the Levant (ISIL) have only asymmetrical capabilities, some of there quite significant. Another group of states, including India and Australia, as well as two major politico-military organizations - NATO and the EU - have policies and means of enforcement that cover, to some extent, the entire spectre of unconventional aggressions.

If the Russian Federation has already begun to implement hybrid strategies, doctrines and tactics, we ask ourselves the natural question why the West seems to have lagged behind in this area and what it could do to reduce the discrepancy between it and Russia's advance in using this type of aggression.

Theoretically, the concept of hybrid warfare has emerged and has been debated in the American literature, being taken over and adapted by European specialists, especially after the crisis in Ukraine. It should be noted that, although not as such, it was studied and analyzed before the Ukrainian crisis by Russian military theorists. So, the development of the concept evolved unnaturally, meaning it was limited to the level of each school of thought. However, the hybrid war remains a theoretical concept launched in the United States after the 2006

Lebanon conflict and whose theoretical value has been highlighted in the literature after the protest movements in the Middle East and North Africa since the early 2010s, known under the name of "*Arab Spring*", when the Russian military theoretical school assimilated, in the category of lessons identified and learned, the mode of action of the West in the Middle East, while the European school mainly looked towards the aggression of Russia in Ukraine and the danger represented by terrorism and migration.

In this context, focusing efforts on specific theoretical concepts or related to modern warfare is more than necessary to understand the evolution of hybrid conflict theory. Increasing the degree of understanding of the hybrid concept can be achieved through a brief analysis, even comparative, of the theoretical approaches specific to each school - Western and Eurasian - focused on the components of the war, such as the nature of the aggressor, the objectives targeted, the tactics, techniques and procedures (TTP) used, the approach towards confrontation and counter strategies.

Hybrid type actions in the Western vision

Even though the term '*hybrid warfare'* was first introduced in the text of the NATO Summit Declaration in Wales on 5 September 2014, references about hybridity have generated much debate and even controversy, especially in the US. Therefore, we will begin the analysis of hybrid actions in the Western vision with American military thinking, but we will also refer to some allied states (Great Britain) or partners (Sweden).

Western organizations (NATO, EU)

Major changes in the physiognomy of conflicts prove that maintaining national security exceeds the capacity and area of responsibility of a single country, even an organization. Moreover, security can no longer be guaranteed by the strict application of military power alone, but by a comprehensive conceptual approach and a new intensity of civil-military actions, including unconventional TTP's in order to achieve strategic objectives. From this perspective, some authors[1] consider that a systemic and multilateral approach of the adversary is required, such the PMESII model (Political, Military, Economic, Social, Information and Infrastructure, especially the critical one).

NATO

The influence of American military concepts exercised directly or through the North Atlantic Alliance, has inspired numerous analyses, debates and conferences, fueled opinions and substantiated key decisions on military doctrines, organization and use of Armed Forces of the allied states and partners. The takeover of American models has undoubtedly contributed to the development of inter-operability between the armies of NATO member states, an essential condition for success in the case of real missions. Without being an exception, the translation of the concept of hybrid warfare from the space of American doctrinal debates into the content of NATO operational concepts, of the armies of the Member States, of partners and beyond, confirms once again the force of attraction of the military theories of American origin.

A first attempt by NATO to define this new type of threat occurred in 2009, at the Supreme Allied Command for Transformation (HQ SACT), when the hybrid threat was described as "*perceived by any established or potential adversary, whether it is non-state or terrorist states or actors, who have the ability, demonstrated or probable, to use both conventional and unconventional means simultaneously and in an adaptable way to achieve their stated goals*".[2]

[1] Crăişor-Constantin Ioniţă, *Potential national measures to counteract hybrid forms of war*, in The Romanian Military Thought magazine no.2, April-June 2015, The Romanian General Staff publishing house, Bucharest, pp. 25-26.

[2] *** *Multiple Future Projects. Navigating towards 2030. Findings and Recommendations*, NATO Allied Command Transformation, Apr. 2009.

The influence of American concepts regarding the hybridity of the contemporary conflicts is evident in the Allied Joint Doctrine, promulgated on December 21, 2010 by the NATO Standardization Agency, according to which the analysis of the current security environment confirms "*the existence of numerous arguments in favor of continuing the process of blurring the boundaries between state and non-state actors (insurgent, terrorist or criminal groups), leading to the conclusion that NATO could face adversaries capable of using both conventional and unconventional means. Threats could be compound, when the actors exercising them act unsynchronised and uncoordinated, or hybrid when implemented simultaneously and coordinated by a particular adversary.*"[3] This doctrine takes into consideration a possible exploitation of NATO vulnerabilities by some adversaries able to resort to difficult-to-anticipate hybrid threats, without complying with Western legal and ethical norms, for achieving long-term strategies focused not on gaining victory but on avoiding defeat.

The NATO *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation* approved at the Lisbon summit on 19 November 2010 shows that, to a degree, the Alliance has adapted to the new risks and threats, but has certain limits as well. The positive elements include the confirmation of intent on the part NATO member states to pursue collective defence in the face of an attack, "*including against novel threats*". Among these threats against the Alliance, the following were quoted – nuclear aggression, terroristic, criminal and cybernetic. The big gain of this strategic concept is to emphasize the crucial importance of developing NATO capabilities in the cyber domain, which has become the new "*star*" of budget allocations in the US and in NATO member states. The negative part is the absence, almost entirely, of the Alliance's declarative concern regarding the informational, psychological, media, cultural, religious, image-based and symbolic aggressions in the moral domain that is the category of risks and threats based on *soft* means. It can be assumed that this burden was left on the shoulders of nations, individually, to undermine the perception of the other great powers (Russia and China), but the lack of coordination in the mentioned areas creates a vulnerability for the Alliance, including through its internal erosion, as demonstrated in recent years with the launch of the Kremlin's propaganda offensive.

The American perspective on hybrid warfare is transposed into articles and messages by Alliance officials, saying that "*hybrid threat is an umbrella concept*", which includes "*a wide variety of hostile circumstances and actions, including terrorism, migration, piracy, corruption, inter-ethnic conflicts etc.*"[4] Conventional (states) as well as non-conventional (asymmetric and non-state) actors can generate hybrid threats through dissimulation of their hostile intentions and referring to hidden actions and through *proxies*, by unidentifiable forces or attributing a false identity, capable of acting for a long time under adverse conditions. Complementary to the classic application of armed force, the hybrid war refers a variety of non-military instruments used in a coordinated manner before, during and after the real military actions.

The very mention of the concept of hybrid war in the declaration of the NATO summit in Wales (2014) testifies to the considerable influence of American military thinking at the level of the doctrinal debates of Allied Commands and the transatlantic circulation of ideas, terms and definitions, as well as their transition from scientific research to experimentation and implementation in NATO exercises and operations. Besides, the characteristics of American concepts regarding hybrid threats and warfare were reflected in NATO documents before the adoption of the Summit Declaration in Wales. In this regard, the activity of the NATO Working Group for Strategic Planning and Concepts is quite relevant, since, in February 2010, it defined the hybrid threat as "*the one that occurs from any adversary,*

[3] *** *Allied Joint Doctrine AJP-01 (D),* NATO Standardization Agency (NSA), december 2010, pp. 2-6.

[4] Michael Aaronson, Sverre Diessen, Yves de Kermabon, Mary Beth Long, Michael Miklaucic, *NATO Countering the Hybrid Threat,* PRISM, A journal of the Center for Complex Operations, vol.2, nr.4, 09/2011, p. 115, https://www.jstor.org/stable/26469152?seq=3#metadata_info_tab_contents accesed Febryuary 21, 2020.

current or potential, states, non-state entities and terrorist group, which has the ability, demonstrated or probable, to use both conventional and unconventional means simultaneously and adaptively in order to achieve their own objectives".[5]

The NATO Summit Declaration in Wales mentioned:

- *The essential characteristics of the hybrid war* (coordination, synchronization and superior integration of the military operations with the actions of the paramilitary forces and the support activities carried out by the civil institutions and agencies at political, diplomatic, economic and informational levels, before, during and after the end of the armed conflict);
- *The objectives of the hybrid type conflict* (increasing NATO response capacity, the need to equip Alliance members with the most appropriate tools for preventing and countering hybrid threats, implementing the Alliance Action Plan for increasing operational capacity - Readiness Action Plan);
- *The lines of action* (improving information exchange, improving political consultation processes and internal coordination to strengthen NATO cooperation with other organizations and optimize strategic communication and elaborate NATO exercise scenarios based on the particularity of specific hybrid war threats).

NATO's concept of hybrid warfare represents the shift from the classic approach of conducting military actions to a comprehensive approach, which combines military and non-military means in the campaigns conducted so as to allow the state that employed them to deny direct involvement. Indirectly, but closely related to the hybrid type conflict, there are other concepts when we refer to the operational side of the hybrid warfare, among which the *informational war*, *lawfare* (the use of national and international law in other ways than those provided by the creator to achieve strategic or political military objectives) or the *4th generation war* (the disappearance of the boundary between war and politics, combatants and civilians).

For the current security situation, but also for the future, some Romanian analysts[6] appreciate that NATO is able to reconfigure its general approach to simultaneously respond to all challenges by: *discouraging* threats from hostile states, *isolating* threats from non-state entities, *protecting and defending* the infrastructure and territories of its member states, the lines of communication and the common goods. The new hybrid threats will no longer be countered by masive armies, created by methods and procedures that belong to the past (compulsory military service and / or mobilization), but the need for deterrence, both nuclear and classical / military, will be kept in order to reduce the effectiveness of terrorist threats and weapons of mass destruction on the part of the opponent. Deliberately, the current conflicts no longer tend towards the complete destruction of the enemy, being more convenient to *buy* it, compared to its destruction by costly action, with numerous victims on both sides. The logic of a total war must yield in favor of a limited war, very similar to the economic one.

Given the complexity of the hybrid conflict, the Alliance member states and NATO as a whole are facing the need to identify new solutions to counteract these new TTPs applied by Russia in Ukraine, which rely on "*creating fear for similar actions in other parts*"[7]. At Alliance level, counteracting hybrid threats is a permanent concern for realizing a concept regarding military contribution in order to counteract these threats and the allied ability to respond to the challenges and risks associated with hybrid warfare, speed of reaction / response, informational operations, cyber domain, social groups that can be used as targets / tools and critical infrastructure issues.

[5] *** *Hybrid Warfare: Briefing to the Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Services*, p. 15.

[6] Florian Ianoşiu Hangan, Marcel-Petru Ivuţ, *The strategic directions of action of the Alliance and its adaptation to the new models of military operations*, in The Romanian Military Thought magazine no.3, July-September 2015, The Romanian General Staff publishing house, Bucharest, 2015, p. 142.

[7] John Blau, *Russia's Periphery: Who's Next?*, Deutshe Welle, March 20, 2014, URL: https://www.dw.com/en/russias-periphery-whos-next/a-17509323 accesed Febryuary 21, 2020.

We can see that some important Member States are adapting more slowly to the current security environment compared to the US or its traditional rival, Russia, as follows: Germany announced in 2015 a new *Security Policy White Paper*, the old one being in force since the year 2006, and the defence policy was enacted in 2011, while France revised its *White Paper on national defence and security* in 2013. Also, the programmatic document in the United Kingdom security and defence field, updated at the end of 2015 and titled *National Security Strategy and Strategic Review of Defence and Security 2015. A safe and prosperous United Kingdom* refers to "*more aggressive, authoritarian and nationalist behavior of Russia*" and its use of hybrid tactics in order to undermine international standards of cooperation, so that it can secure its own interests.

European Union

Compared to NATO, the EU is far from approaching the hybrid domain, and the Union's security policies need major corrections to become viable, although there is already awareness of this type of threat or aggression. On 6 October 2015, the President of the European Council, Donald Tusk, pointed out that "*gradually we are witnessing the birth of a new form of political pressure, and some even speak of a new type of war, a hybrid, in which migratory waves become a tool, a weapon for the neighbors. This requires a great deal of sensitivity and responsibility on our part*"[8].

The contribution of the European school to the development of the hybrid concept comes, with small exceptions, from the area of British and Swedish schools, being late and in direct relation with the evolution of, and the level of perception regarding, the security risks and threats manifested in the European space, where the Russian threat occupies a central place. In a larger vision, which is not specific to the Russian model, the European approaches claim that hybrid aggression is limited to the combined, synchronized, simultaneous and innovative application of conventional (military) and unconventional (political, diplomatic, economic, informational) means, available for a state or non-state entity in order to reach a certain strategic objective proposed in relation to another actor, whose vulnerabilities are exploited and whose centers of gravity are attacked (political, economic, military, social information).

The theoretical model of hybrid warfare developed by Erik Reichborn-Kjennerud and Patrick Cullen (2015) is perhaps the most representative way to illustrate the European approach to hybrid warfare, which "*is characterized by the appropriate use of all power tools on the vulnerabilities of the opponent*".[9] In the model described by the two autors, the notion of hybrid is not limited only to the means and power tools and their combination to achieve the set objective, but also to the way in which they are used and to the coordination and synchronization functions for achieving synergistic effects regarding purpose, the synchronization emphasizing the multiplicative effect of hybrid aggression.

The thesis of the American F.G. Hoffmann, on the "*uniqueness of hybrid warfare*", is taken over and developed by the European school. Between the context in which the confrontation between two actors and the strategic options of the aggressor there is a direct conditionality, since the context and the multitude of causes that determine it are unique. This makes the way in which the means and the power tools are combined in hybrid aggression unique in every single instance.

As an argument that supports the prevalence of non-military means and methods in the hybrid type conflict, another component of the threat manifestation - *lawfare*, an older and reinvented American concept in the context of the crisis in Ukraine - is highlighted in the European literature. In a more simplistic view, it designates a form of war that consists in using the legal system (national and especially international) against an enemy to delegitimize

[8] Donald Tusk, *Valul de refugiaţi este un război hibrid împotriva Europei*, agenţia Agerpres, Bruxelles, 07.10.2015.

[9] Erik Reichborn-Kjennerud, Patrick Cullen, *What is Hybrid Warfare?*, Norwegian Institute for International Affairs, Policy Brief 1/2016, p. 3.

him. Lawfare is associated with a "*strategy for using or circumventing the law, that substitutes military means for achieving a certain operational objective*"[10], the best example being the Russian interpretation of the allegations regarding the violation of the Budapest Agreement (1994), which regulates independence and the sovereignty of Ukraine, by annexing the Crimean peninsula. The official position of Moscow from that date (April 2015) was that the Budapest Agreement provided, in addition to guaranteeing independence and sovereignty, the abstention from threatening Ukraine's political independence, and "*Russia did not oppose the will of the Crimean population who expressed its esire for a return to the Russian Federation*"[11].

Among the approaches that refer to hybrid actions which were developed before the Ukrainian crisis, the Swedish one should be noted. In the autumn of 2012, an exercise was performed for the first time in Sweden based on a scenario running on the hybrid concept of modern warfare.[12] The exercise scenario provided that an imaginary enemy (an island in the Baltic Sea whose relations with neighboring states, implicitly with Sweden, have been significantly damaged) is carrying out a series of actions in order to destabilize the Swedish state, such as cyber attacks against governmental IT systems, threats to a high-ranking Swedish government official, the destruction of a turbine at a nuclear power plant by infecting its command-control system with a computer virus (similar to the Stuxnet virus used in the Iran attack in 2010), the dislocation of a group of Special Forces operators on Swedish territory or employing Somali pirates to hijack Swedish vessels in the Horn of Africa. This latter action illustrates the fact that a local conflict can be fueled by actions carried out over a long distance, in this case the activation of hotspots in the unstable region of the Horn of Africa. The conclusions revealed that the standard operating procedures existing at that time generated an efficient response of the authorities on the types of threats addressed individually, but also the deficiencies of trying to counter the complex threats caused by the absence of a national strategy defining an integrated and inter-departmental approach.

Hybrid type actions in Eurasian conception

The elements promoted in the theoretical model of hybrid war of American conception find their correspondence also in the ideas produced by the Russian military school of thought. What makes this situation possible is precisely the premise from which we must start in researching the hybrid concept - conflict of this kind has always existed and is currently the most advanced in the practice of modern warfare, and not a new type of warfare in the true meaning of the word.

Russian-speaking media from Eurasia, a vast territory that mainly represents the territory of the Russian Federation and the former component republics of the former Union of Soviet Socialist Republics (USSR), or the so-called "*-stans*", presents the hybrid war as a military strategy that combines conventional warfare tactics with new generation, cybernetic means and techniques. In this part of the world, the Russian perspective of the 21st century warfare prevailed over others, but it is surprisingly much like the Western concept of the hybrid conflict, resulting from the annexation of the Crimean Peninsula and the clashes between the Ukrainian armed forces and pro-Russian separatists in the self-proclaimed Donetsk and Lugansk People's Republics.

On the other hand, the increased interest of Russian military theorists towards the concept of hybrid warfare (in Russian "*gibridnaya voyna*") is due to the intensification of

[10] Charles J. Dunlap Jr., *Law and Military Interventions: Preserving Humanitarian Values in 21st Century Conflicts*, Humanitarian Challenges in Military Intervention Conference, Carr Center for Human Rights Policy Kennedy School of Government, Harvard University Washington DC, November 29, 2001.

[11] John Moore, *Lawfare,* The Three Swords Magazine 31/2017, p. 38, http://www.jwc.nato.int/images/stories/_news_items_/2017/Lawfare_Moore.pdf accesed February 21, 2020.

[12] Sacha-Dominik Bachmann, Hakan Gunneriusson, *Hybrid wars: The 21st-century's new threats to global peace and security*, May, 2015, pp. 28, 80, https://www.researchgate.net/publication/307831898_HYBR accesed February 21, 2020.

debates in the US military environment. In order to conceptualize the term *hybrid*, Russian military analysts have focused on understanding and applying Western / American theory but from the Russian perspective of the phenomenon of war. Thus, the Russian interpretation of the hybrid war involves all domains of social life (politics, economy, culture, etc.), as opposed to the American approach which is reduced to combat actions, largely at the tactical and operational levels.

From a Chinese perspective, although the primary source of the hybrid concept is considered the work of Qiao Liang and Wang Xiangsui, *Unrestricted War*, launched in 1999 by the People's Liberation Army (PLA), there is currently not much data about the Chinese military's research in the field. Because there are no translations of the work of the two Chinese authors, the vast majority of Western works use James Perry's article in the Aerospace Power Journal, published in the summer of the year 2000, as a reference point. According to J. Perry, who based his appreciation on the laudatory comments on the book in the official publications and on the fact that *Unrestricted War* was published by the PLA's official publishing house, the work of the Chinese military experts enjoyed the support of the Chinese military-political leadership. "*Later, the Western press quoted various sensational passages from the book and described it in terms that bring it closer to a hyperbole, but the work of the two Chinese authors was not a plan for a dirty China war against the West, but an appeal to an innovative thinking about the future of war*", said J. Perry**.**[13]

Eurasian organizations (CIS/CSTO)

The Commonwealth of Independent States (CIS) emerged after the disintegration of the USSR (1991) as a continuation of cooperation between the former Soviet republics and, as the name implies, constitutes a union of states based on common historical values and links but, according to the definition given by the Organization for Economic Cooperation and Development (OECD), it also represents an international body "*established by formal political agreements between their members that have the status of international treaties; their existence is recognised by law in their member countries*".[14] The purpose for which the CIS was established, as stipulated in the Charter of the organization, is the multilateral cooperation (political, economic, social, cultural, etc.) and, although it was reached the creation of a Eurasian Economic Union (EEU), which would provide economic growth for all member countries, only 5 of the 9 former member states of the Community, Belarus, Kazakhstan, Kyrgyzstan, Russian Federation, Armenia, are also in the Eurasian Economic Union.

In order to ensure its own defence system, CIS established the Treaty on Collective Security (TSC), according to which the security of the Member States is based on the principle of collectivity, similar in some way to art. 5 of the North Atlantic Treaty: "*in case of aggression against any Member State, all other Member States will provide all necessary assistance, including military support, and at the same time support it with all available means for the implementation of collective defence rights as stipulated by Article 51 of the UN Charter*"[15].

In 2002, the TSC becomes an organization – the Collective Security Treaty Organization (CSTO) - and later, in 2004, it is internationally recognized by the UN and receives observer status at the General Assembly of the Organization.

[13] Iulian Chifu, *Hybrid Warfare, Lawfare, Informational Warfare. The wars of the future*, International Scientific Conference Strategies XXI, Complexity and Dynamism of the Security Environment vol.1, Center for Strategic Defense and Security Studies, "Carol I" National Defense University publishing house, Bucharest, 2015, p. 203.

[14] *** *OECD Glossary of Statistical Terms*, Organization for Economic Cooperation and Development, https://stats.oecd.org/glossary/detail.asp?ID=1434 accesed February 21, 2020.

[15] Anatoliy A. Rozanov; Alena F. Douhan, *Collective security Treaty Organization 2002-2012*, DCAF Regional Programmes, Geneva-Minsk, 2013, p. 4, https://fir.bsu.by/images/departments/ir/ir-materials/ir-studyprocess/Rozanow/Rozanov%20A.,%20Douhan%20A._RPS_18_CSTO_2002-2012_DCAF%202013.pdf accesed February 21, 2020.

In order to also have a power tool, the OTSC set up in 2009 the Collective Rapid Response Force (CRRF) to counter both traditional and unconventional military threats, such as emergency situations. The level of ambition was similar to NATO, in that it wanted CRRF to be as well-equipped and efficient as those of the North Atlantic Alliance, including in the hybrid field.

Contrasting the two major military blocs, the CSTO representing the East and NATO for the West (but mainly the two leading states: Russia and the US), and considering the policies, strategies and objectives of their member states, Dr. Alexandra Sarcinschi states that, unlike the countries of the North Atlantic Alliance, where there is a common approach to security issues involving the member states of the Organization, in the case of CSTO there are different approaches of its members to NATO / USA. For example, Russia has included in its national strategy the danger posed by NATO, but other CSTO countries have chosen to cooperate militarily with the US, as the leader of the Alliance. If, in the case of CSTO member countries, the strategic conception is built around the idea of collective security, the specific elements of NATO's strategic conception are found in most of the national strategies of the members: collective defence, crisis management, security through cooperation and non-article 5 operations.

NATO and CSTO do not have consistent points of cooperation. Although the Alliance is interested in the security situation in the center of the Asian continent, and some CSTO member countries are part of the NATO Partnership for Peace, the dialogue between the two organizations is limited. In addition, representatives of the organization are beginning to bring to the attention of the public the fact that the CSTO will try to strengthen the collaboration relations with China, including the Shanghai Cooperation Organization (SCO).

As Russia, as heir to the former USSR, holds the monopoly of regional cooperation and collective security organizations in Eurasia, respectively CIS and OTSC, Russia's national security strategy and military doctrine are a model for the other member countries.

Also, the lack of information or scientific studies on the issue of hybrid warfare in the Chinese vision has led us to deepen the research of hybridity in the vision of the Russian school, which we consider representative for the Eurasian space.

The Russian Federation

Following the study of the evolution of the concept of hybrid conflict in Russia, the US military analyst of the Office for Foreign Military Studies at Fort Leavenworth (Kansas, USA), Timothy Thomas, appreciated that the conceptual development of the hybrid concept in Russian military thinking was accomplished in three stages: studying the American school and integrating the lessons learned for Russia, the certification of the *new generation war* by the Russian Military Academy and the accreditation of the *new type of war*, a product of the General Staff of the Russian Armed Forces.

In a *first phase*, Russian military theorists studied the American concepts of hybridity, the most representative paper for this period being the article published by the head of the Russian General Staff, Gl. Valeri Gherasimov, in the Military-Industrial Courier no.8 of 2013, entitled *The value of science in prediction*, work taken, commented and analyzed by numerous Western publications and receiving the generic name of *Gherasimov doctrine*. In this article, Gl. V. Gherasimov points out that the trends in the conduct of war are in a continuous dynamic change and underlines the need to return to military science, and the Russian military academic environment is responsible for identifying innovative, applicable and usable ideas at the level of the Russian political-military leadership.

However, in order to highlight the continuous transformation of the character of the war, Gl.V. Gherasimov recalls the 1933 work of the professor at the Russian Military Academy, Col. George Isserson, entitled *New forms of combat* and in which he appreciated, contrary to the current era, that "*war, in general, is not declared. It simply starts early with the deployment of the armed forces. The mobilization and concentration of forces does not refer to the period after the declaration of the state of war, as it was in 1914, but they are* *gradually realized, unobserved, long before that*"[16]. In his turn, Gherasimov concludes that, „*in the 21st century, the tendency to erase the differences between the state of peace and the war continues to manifest. Already the wars are no longer declared and, once they have begun, they are no longer in accordance with an established model*"[17].

In the content of his article, Gherasimov highlights the danger represented by the "*colored revolutions*" in the so-called *Arab Spring* (2010), for which the West is responsible, and refers to NATO operations in Libya since 2011, among which he recalls the establishment of a no-fly zone, the imposition of a maritime blockade, or the use of civilian contractors in the battle against armed opposition (Russia will later use private Russian security companies in Syria, such as the Wagner Group). All of these actions are considered an example of the modern warfare and point out the main trends of change in the contemporary warfare: wars are no longer declared and once initiated they unfold after an unfamiliar pattern (blurring the border between peace and war); an increase in the relevance and the role of non-military resources for achieving strategic political and military objectives; military means are used to dissimulate, and regular forces are used in sight only to force the fulfillment of the proposed goals and most commonly under the pretext of peacekeeping operations.

Due to the difficulties in anticipating the characteristics of future military conflicts, Gherasimov stresses the importance of the predictive function of military science and recommends studying the new types of threats and wars by examining atypical approaches at the Russian Military Academy and General Staff. The fact that modern wars are not declared and are not legally assumed by the parties involved requires a different kind of analysis about the circumstances in which they arise, which must take into account the provisions of national and allied laws, strategies and doctrines, the observance of the norms of international law in opposition to the realities of the battlefield, whose dimensions exceed the simple military confrontation through the use of political, diplomatic, economic, informational or humanitarian means and resources.

In the *second stage* of Russian hybrid research, the ideas of Gl. Gherasimov are adopted and developed by the Russian Military Academy. The model of the new generation war, proposed for debate in 2013 by Gl.lt. (ret.) Sergei A. Bogdanov and Col. (r.) Sergei G. Chekinov, shows some similarities with the American theory of hybrid warfare and can be considered a precursor to the model of the new type of war, later supported and promoted by the Russian political and military leadership. In our opinion, the elements described by Chekinov and Bogdanov have a high practical-application value at all levels (strategic, operational and tactical). In general, the two authors point out that the war of the new generation will be dominated by informational and psychological operations to discourage the adversary's forces and population. At the same time, the indirect approach and the asymmetrical / unconventional actions will prevail in front of a superior adversary from the military point of view, an aspect reflected in the accentuation of the use of non-military means (political, economic, informational, technological, cybernetic) and their combination to maximize the effects.

At the beginning of 2015, the thesis of the new type of war, based on the integration of lessons learned from the conflicts in which the Western states were involved, in the Middle East and North Africa, was explained by Gl.lt. Andrei V. Kartapolov, former head of the Operations Directorate of the Russian Joint Chiefs of Staff and former head of the Western Military Region. Although its approach has to be looked upon with reservations due to the functions it holds and the strategic geopolitical context, marked by the escalation of tensions between Russia and the West after the annexation of the Crimean Peninsula (March 2014), some aspects can be considered useful in determining the Russian view on the new type of war. Broadly speaking, the new type of war represents "*80-90%, propaganda and 10-20%, violence*", and "*the use of the methods specific to the indirect approach leads to the*

[16] Valeri Gherasimov, *Valoarea ştiinţei în previziune (Ţennost nauki v predvidenii)*, în Curierul militar-industrial (Voenno-Promîşlennîi Kurier), nr.8 (476), 2013, p. 3.
[17] *Ibidem*, p. 2.

achievement of military objectives without necessarily having to employ regular forces"[18]. In other words, in the new type of war imagined by Kartapolov, the indirect actions conducted by a state against the enemy will predominate, concentrated on the informational dimension of the confrontation - in the political, economic, informational, cybernetic and psychological environment of the target and in the international community, where political-diplomatic and propagandistic actions prevail - the classical means of conducting the (military) war being taken into account only in the escalation phase of this step.

In the *last period*, the new type of war was accredited, a moment marked formally by the publication of the new military doctrine of Russia (December 2014), in which most of the ideas Gl. Gerasimov are reflected. The new Russian Military Doctrine identifies the risks and threats to Russia and the possibilities of counteracting them, including by non-military means (political, economic, etc.), the characteristics of contemporary conflicts, the conditions that could determine Russia's involvement in a war and the intensity of the response, the types of operations and how the Russian armed forces should engage in combat, the needs for economic support or the requirements of developing cooperation within international organizations, strategic partnerships and bilateral relations.

Modern military conflicts benefit from a detailed description in the new Russian military doctrine, and the characteristics and particularities that Russian military theorists attribute to them are similar to those of the followers of the hybridity of contemporary wars.

Conclusions

The approaches and interpretations of the hybrid concept of the Euro-Atlantic and Eurasian schools of thought are complementary, the differences between them contributing to the development of the concept even if they have generated some confusion regarding the terms being used. Each of the analyzed schools (Western and Eurasian) approaches the problem of hybrid warfare from the perspective of the opponent, regardless of the nature of his actions, thus restricting the meaning of the war to the threat. To eliminate this kind of confusion, it would be beneficial to differentiate between concepts that can be attributed exclusively to the adversary - hybrid actions or hybrid threats - and those that describe the hybrid nature of the confrontation. Approaching the hybrid conflict only from the adversary's perspective creates the impression that the aggressor is permanently on the offensive, while the opponent is in a permanent defensive state. But the war describes a dynamic process, in which the two forms of manifestation of combat actions, offensive and defence, alternate. After all, hybrid warfare is nothing more than the transposition into practice of one party's intentions / will over the other (as in Von Clausewitz's classic vision), intentions that until the moment of escalation were perceived as threats.

In general, the purpose (objectives) of the actions associated with the hybrid conflict is presented by these schools in the general way, in principle the theory is that the actors who utilize a hybrid type of action pursue the achievement of ideological goals - in the case of non-state entities - or politico-military - in the case of state actors. If the aggressor is a state, we find that the military / violent side of the confrontation does not prevail, but most actions take place in the immaterial plane of knowledge. In this sense, the Russian specialty literature introduces the term adaptive approach to the use of force, usually armed, by which we understand the use of conventional forces and capabilities (gradually and in different forms), from the dissimulated use of own forces (under the mask of some activities for training the opposition forces and hidden missions of the Special Operations Forces) all the way to their involvement in military actions in sight (according to Gl. Gherasimov, the ratio of forces would be 1 to 4 in favor of non-military means). The action strategy integrates the methods / courses of action and the means / resources that can be used for the successive achievement of specific / partial / phase objectives, which will ultimately contribute to achieving the proposed political objectives.

[18] *Ibidem*, pp. 31, 33.

Most of the theories on hybridity in the specialized military literature contain descriptions of the terms and less those aspects that refer to how to counteract hybrid actions. Usually, the authors use the model of the American school about the hybrid war or reiterate the lack of novelty of this type of conflict, the proposed definitions being quite unclear or confusing and very general, while missing a well-defined demarcation line between the concepts used - hybrid threats or hybrid actions.

In conclusion, the analysis of the two schools, Western and Eurasian, shows us the preference of theoreticians from both sides for the study of concepts and hybrid type confrontation from a military perspective, by emphasizing the changes in the physiognomy of the war, especially at the operational and tactical levels, caused by the shifts in the operational environment.

However, in contrast to the American and Russian approaches, references to hybrid warfare in the European space mainly focus on the side of hybrid threats, with an emphasis on the informational and cyber dimensions mainly generated by state actors, but also on their response and counteraction.

BIBLIOGRAPHY

1. AARONSON, Michael; DIESSEN, Sverre; KERMABON, Yves de; LONG, Mary Beth; MIKLAUCIC, Michael, *NATO Countering the Hybrid Threat,* PRISM, A journal of the Center for Complex Operations, vol.2, nr.4, 09/2011;
2. BACHMANN, Sacha Dominik; GUNNERIUSSON, Hakan, *Hybrid wars: The 21st-century's new threats to global peace and security,* May 2015;
3. BUŢA, Viorel; VASILE, Valentin, *New type of war: Russian perspective*, in the Romanian Military Thought magazine no.2, April-June 2015, The Romanian General Staff publishing house, Bucharest, 2015;
4. BLAU, John, *Russia's Periphery: Who's next? ¸* Deutshe Welle, March 20, 2014;
5. CHIFU, Iulian, *Hybrid Warfare, Lawfare, Informational Warfare. The wars of the future*, International Scientific Conference Strategies XXI, with the theme Complexity and Dynamism of the Security Environment, vol.1, Center for Strategic Defence and Security Studies, „Carol I" National Defence University publishing house, Bucharest, 2015;
6. DUNLAP, Charles J. Jr., *Law and Military Interventions: Preserving Humanitarian Values in 21st Century Conflicts*, Humanitarian Challenges in Military Intervention Conference, Carr Center for Human Rights Policy Kennedy School of Government, Harvard University Washington DC, November 29, 2001;
7. IONIŢĂ, Crăişor-Constantin, *Potential national measures to counteract hybrid forms of war*, in the Romanian Military Thought magazine no.2, April-June 2015, The Romanian General Staff publishing house, Bucharest, 2015;
8. HANGAN, Florian Ianoşiu; IVUŢ, Marcel-Petru, *The strategic directions of action of the Alliance and its adaptation to the new models of military operations*, in The Romanian Military Thought magazine no.3, July-September 2015, The Romanian General Staff publishing house, Bucharest, 2015;
9. MOORE, John, *Lawfare*, Three Swords Magazine 31/2017;
10. REICHBORN-KJENNERUD, Erik; CULLEN Patrick, *What is Hybrid Warfare?* Norwegian Institute for International Affairs, Policy Brief 1/2016;
11. ROZANOV, Anatoliy A.; DOUHAN, Alena F., *Collective security Treaty Organization 2002-2012,* DCAF Regional Programmes, Geneva-Minsk, 2013;
12. SARCINSCHI, Alexandra, *Politics, strategies, strategic objectives - a comparison between West and East*, in the Romanian Military Thought magazine no.1, January-March 2016, The Romanian General Staff publishing house, Bucharest, 2016;

13. THOMAS, Timothy, *The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking*, The Journal of Slavic Military Studies, vol.29/issue 4, 2019;
14. TUSK, Donald, *The wave of refugees is a hybrid war against Europe*, Agerpres news agency, Bruxelles, October 10, 2015;
15. *** *Allied Joint Doctrine AJP-01 (D)*, NATO Standardization Agency (NSA), December 2010;
16. *** *Hybrid Warfare: Briefing to the Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Services*;
17. *** *Livre Blanc Défense et Sécurité Nationale – 2013*, Paris, April 2013;
18. *** *Military doctrine of the Russian Federation (Военная доктрина Российской Федерации)*, p.5, in Rossiyskaya Gazeta - Federal Issue nr.6570 (298);
19. *** *Multiple Future Projects. Navigating towards 2030. Findings and Recommendations*, NATO Allied Command Transformation, aprilie 2009;
20. *** *National Security Strategy and Strategic Defence and Security Review 2015. A Secure and Prosperous United Kingdom*, HM Government, noiembrie 2015;
21. *** *OECD Glossary of Statistical Terms*, Organization for Economic Cooperation and Development;
22. *** *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation*, adopted by heads of state and government at the NATO summit in Lisbon, November 20, 2010.

NATO'S NEW PLANNING PROCESS – FROM THE STRATEGIC TO THE OPERATIONAL LEVEL

Petre LUCA
"Carol I" National Defence University, Panduri, București, România
luca.petre.georgel@gmail.com

Abstract: *The Comprehensive Operations Planning Directive - COPD hinges on two principles: comprehensivity and proactivity. These drivers set the scene for better and more realistic operations planning. However, without a mature understanding of the process, the experience of participating in an operational planning group at any of the strategic, operational or tactical levels, can be an unsatisfying and pointless experience. This paper explains the interrelationships between the strategic and operational level and offers ways to avoid the traps that sometimes the COPD lay against us.*

Keywords: *operational planning, joint, center of gravity, factor analysis, assumptions, war gaming.*

Introduction – a short walk through strategy

In a strict sense, the strategic estimate is a continuous assessment of factors that influence the determination of missions, objectives, courses of action and addresses mainly the military domain as an instrument of power. In a much broader sense, the strategic estimate is a cognitive process that deals with analyzing the way forward for an organization, establishing its core conceptual elements, the mission, vision and values as well as the functional elements, ends, ways and means. While strategy rest in the past in the military domain, the recent developments in the sociopolitical realm pushed for a pervasive adoption of it.

One such development, the globalization, required leaders in the economy domain, to enlarge their perspectives in order to grow their companies. Producing and selling to a local market, requires a minimum effort of vision and planning as it mainly responds to client needs in a peer-to-peer mode. The manufacture of goods for a global market, however, requires a deep strategy which includes controlling the supply chains, conducting marketing campaigns as well as employing or using a logistic footprint.

In the informational domain as well, the necessity to protect the networks, lead to a protracted fight against a plethora of threats ranging from the physical to the software security. The permanent escalation of this conflict required a development strategy in order to provide sustainable growth of the networks. However, the most recent developments providing cyber-attack capabilities, require also a coherent and coordinated approach in order to achieve the proposed aims. Moreover, in this domain, exposing one's vulnerability triggers a rapid reaction of the adversary in remedying it thereby closing very fast the window of opportunity for subsequent attacks. This is literally "*one shot*" option requires a tremendous amount of effort in assessing the actions as to obtain maximum of effect of the fleeting opportunity.

One other development that influences strategy is the emergence of the hybrid conflict. This is by no means a tactical endeavor or a way to fight, although too many times identified with little green men, but the usage of the whole range of instruments of power, employed both in conventional and unconventional ways against the opponent. It also requires strong national leadership dominating the whole instruments of power spectrum (Russia) and fits less with political-military alliances that are bound to respect the diplomatic agreements, have a limited control over multinational business or informational environment vectors such as mass-media (NATO). It was the combination of breaking treaties, economic pressure and fake news that kneeled Ukraine into submission.

The changes in the spectrum of conflict is yet another factor that extends the utility of strategy. On one hand the hybridization is stretching the instruments to overlap the spectrum from the peacetime military engagements up to high intensity conflicts. On the other hand, due to technological developments that allow a great degree of control over the tactical units for the higher commands, as well as the necessity to dominate the informational environment, the strategic, operational and tactical levels are compressed this resulting in tactical commanders need to understand the strategic design and contribute to delivering the strategic effects.

The initiation of planning – the strategic estimate

The US doctrine[1] sees this as an analytical product encompassing strategic direction (broad policy, guidance and authoritative direction, requirements, actors' goals and end states), operational environment (areas, adversaries, friendlies and neutrals), an assessment of the major strategic and operational Challenges (from direct military confrontation, peace operations, and security cooperation to providing response to atrocities, humanitarian assistance, disaster relief, and stability activities), potential opportunities (known or anticipated circumstances, as well as emerging situations) and an assessment of risks.

While being no more than an adjusted format of an order this format provides a good overall picture of what military strategic level needs to accomplish in order to contribute to the overall national goals in relationship with the other instruments of power. Most importantly in our view, the strategic estimates remain within the mission command framework which enables the commanders to exercise their leadership.

The UK doctrine[2] sees this more as a process (in line with the 7 questions and the tactical estimates) that enables lower headquarters and units to plan in accordance with the higher echelon. While estimate is being consistent throughout all levels, it is our belief that it greatly impinges in the lower command's freedom of action, by providing them the mission statement.

In great lines influenced by the UK doctrine, the NATO operational planning describes in the COPD mainly the same process, however, with an emphasis on the leader. In NATO's view, the strategic assessment (a synonym of estimate) rests with SACEUR. While it looks good on paper and it is a well-intended initiative for the leaders to own the strategy, in fact the process is ran and the product is delivered through intricate staff procedures that leave less freedom to the commanders to state their intent.

Outside the military domain the term used for a similar process is "*strategic planning*" and implies "*analyzing competitive opportunities and threats, as well as the strengths and weaknesses of the organization, and then determining how to position the organization to best achieve its objectives*"[3].

Although leadership and management are not synonyms, some similarities exist between them and one of them is the process in which the higher authority provides vision and guidance. "*Direction and guidance*" is a well-known and used term in the military community. It suggests that we need a vector and some lateral limits in order to proceed forward. While both relevant, of most importance from our perspective, is the issuance of a leader's vision, which for the higher military levels is only partially covered by the commander's intent. The vision is an integral part of the strategy and provides focus for the

[1] JP 5-0, *Joint Planning*, June 2017, p. II-8.

[2] JWP 5-00, *Joint Operations Planning*, June 2004, p. I-10.

[3] Mason Carpenter, Talya Bauer, Berrin Erdogan, *Management principles,* 2012books.lardbucket.org, 2012.

organization. "*Do more with less for many*"[4] is a vision used both in the NGO environment as well as in the industry. It gives precise vectors for actions (extend and be efficient) as well as implied end state (economic growth). This could easily be transformed into a page worth of words saying the same thing, but the simplicity and the potential to animate of this "*mantra*" is overwhelmingly visionary.

Within the five functions of management (planning, organizing, commanding, coordinating, controlling - Fayol) the first one implies a forecast as the start of the process. Initially in 1916, Fayol named it "*forecast and planning*" and stated that it determines "*what is likely to be required from the organization; opportunities and demands for its services or products, this information helps define the current set of prioritized objectives*"[5.]

Moreover, as with the strategic estimate "*the forecast will have to be constantly monitored and revised. The managers should try to reduce the element of guesswork in preparing forecasts by collecting the relevant data using the scientific techniques of analysis and inference*."[6]

The main conclusion to be drawn from this first part of our paper is that. The strategic estimate and the forecast are similar processes that lay the basis for subsequent planning. They are both higher authority guidance that drives the effort for finding the optimum course of action to achieve the objectives, therefore enabling one of the critical functions of leadership: vision. However, they are used in different domains and suited for their respective purpose. While the strategic estimates provide direction and framework, the forecast focuses on predictions of the future outcomes using statistical operations and calculations as a means to provide a predictive analysis of the anticipated changes.

The focus – the operational level

Operational level planning is currently defined as the "*master of the jointness*". However, the intricate links described in the COPD's operational planning process lead us to believe that an issue cannot be dealt with at a single level, but rather through an all-levels problem-solving approach. The operational level is sandwiched between the strategic and the tactical ones. Building on our recent (international and national) planning experiences based on the new NATO planning methodology, we would like to expand further and share and shed light on several friction points of the process. Although we have tried publishing these on a NATO lessons learned portal, it is now proved that the task could be even more difficult than dealing with them in the planning.

The value of COPD resides in its comprehensiveness. It is its strongest point in the way that not only allows but enforces all levels of planning. In this way, the communication between the planner's communities of different organizations gains momentum thus helping in developing the understanding between higher, lower and lateral headquarters.

All-experts interaction is another major gain. The operational planning groups at all levels have or can rapidly access all expertise that exists in a headquarters. The commanders though, need to understand that this vehicle can be used to plan everything, not only operations and spreading this type of working across the organization, can benefit highly, training or efficiency wise.

The constant update of the Comprehensive Preparation of the Operational Environment - CPOE, even outside the planning cycle, and the perpetuum of the first phase - situational awareness, helps instill a proactive mindset. But these are only the highlights of the

[4] Navi Radjou, Jaideep Prabhu, Simone Ahuja, *Frugal Innovation: lessons from Carlos* Ghosn, CEO, Renault Nissan, hbr.org, 2012.

[5] Wood C. John, Wood C. Michael, *Henry Fayol Critical evaluations in business and management*, Routledge, London, 2002, p. 208.

[6] *Ibidem*, p. 293.

good thing's COPD gives us. The planning, however, works like a washing machine. We put some dirty clothes - factors - in and we should give your lower the clean clothes - e.g. assumptions, tasks, risks; but sometimes the outputs get messed up and we give the dirty water - confusion, uncertainty - instead. The following instances are a few "tips and tricks" to help planners navigate through the operational planning process maze.

Joint planning – think inside the box

Inter-domain or multi-service planning is great. It would be even greater if it would happen, but realistically, every component is trying to cover the entirety of its assigned area and that is a very specific one (land, maritime) or a whole dimension (air, cyber). No matter how hard one tries, the high seas cannot be assigned to a land commander; as much as land cannot be assigned to an air commander. As a result, at the operational level, activities such as course of action development or wargaming, cannot vary largely if the Joint Operational Planning Group - JOPG doesn't account for low-level tactical units. Nevertheless, this could drastically reduce the freedom of action of the component commanders.

Following the experience of applying both methods we can favor the tactical thinking, however, its success depends on the determination of the components' operational planning groups to support the JOPG. If this is not available, then the only thing to do here, is to find and specify those connections where one component can support another - supporting-supported or inter-relationships, or whatever we want to call one service delivering actions or effects to enable another in doing its job better. Besides this, unfortunately, the operational art here goes down solely to integrating effects and synchronizing them in a matrix and/or exchange domain annexes in between components.

Would you risk an assumption?

The favorite word of any planner is "assumption". The planners treat assumptions like pets. They love one, can live with a couple, but try to sell them when they become too many. Usually we push them where they are taking good care of, to "higher status people", meaning in this case the higher headquarters. Up until recently, the targeted organization usually rejected owning assumptions, but lately however, a new behavior appeared. The higher headquarters assume but try to avoid backing-up these assumptions with risks. Any assumption is an empty carton, it looks solid, but it doesn't hold any weight. In order to avoid the plan to crumble, we need to run the risk management process. Assumptions are the main source of the operational risks together with the center of gravity's critical vulnerabilities and factor analysis conclusions. They need to be groomed and handed over not to our higher, but to our lower headquarters for them to be aware of what we identified as potential failures.

Too soon to tell? - commander's guidance

By far the most critical issue that could impede on this process is the late involvement of the commanders in the planning. Through the planning and liaison elements, the headquarters tune up for a better situational understanding and synchronization. Essential parts of the concept of operations (mission statement, objectives, operational areas, force requirements, rules of engagement) are discussed and set well before commanders are available to provide guidance. The planners then struggle to generalize the mission to give their bosses as much coverage as possible for any interpretation they might have.

But this is just one of the two reasons for mission statements becoming half page long, all-encompassing phrases cutting into objectives, commander's intent or even scheme of maneuver. The other one is the top down approach of the mission statement - the mission must be received. However, if the mission statement would not be included in the higher headquarter guidance, but rather, the essential tasks would be directed, then the lower echelon planners and their liaison element would not be put under such pressure. The commander would then be free to state its own mission and still be well within the mission command frame.

The only mitigation to this relies on an early engagement from the senior staff and commander before the actual start of the planning process. The operational planning groups must brief and get a mandate from the commander in order to have a strong and concise input in their higher echelon's planning.

Instruments of power – not that comprehensive after all

With all the comprehensiveness built in the COPD, especially at the strategic level, there is still much to add in the planning. This is because usually, in the strategic planning groups, little if any diplomatic, economic or informational expertise is brought. Most of the time, the military needs to think also for the other instruments of power, although nothing can be based on the rationale that giving a task for the diplomatic or economic level, it will be executed at one point.

Moreover, the strategic plan is the highest level of planning. Therefore, the synchronization of the instruments of power is done by the political level during fierce negotiations. The strategists thus, although militaries, need to think of integrating relevant and achievable instruments of power effects into the overall design.

The factor analysis - derail into detail

Inside syndicates, the comprehensiveness of the group can rapidly turn from a strong point into a weak one. If the facilitators are not experienced enough not only with leading discussions, but also with the subject of the planning, they will not be able to frame the discussions within red – blue - green perspectives of the time-space-forces-information dimensions. Long painful discussions can derail or go into a "rabbit hole", achieving basically nothing of essence. The syndicates can produce tens of factors but then overlook the key ones.

Producing and understanding the CPOE, enlarging perspective with personal knowledge and empowering people that share this knowledge in a proper manner are keys to success in the syndicate rooms.

To COG or not to COG

Just hearing of another process of analyzing a Center of Gravity (COG) has the potential to "hurt" us. It is no surprise when guidance received in the doctrine states "there is no starting point". How can we start a process then?

The key in making a smooth process out of this is first to find out what is "really" critical. The syndicates usually list a series of abilities as critical capabilities, without even considering the opposing COG. Having a great air force is a great capability but does it retain the same level of criticality in an A2AD (Anti-access area-denial) contested environment? To answer this, on one hand, the criticality of capabilities of one's COG need to be tied with the critical vulnerabilities of its opponent, while on another, its own critical vulnerabilities interrupting critical requirements for those critical capabilities, need to be identified. Antagonizing COGs is therefore the method of finding what is truly critical and because we tend to overlook this, much too often, the COG never passes the mission analysis brief into the planning realm. Hence, we do not plan on engaging our enemy's critical vulnerabilities while protecting our own. Ultimately, we need to constantly remember that we must plan on going after the COG but be flexible enough to adapt if the analysis was wrong or the COG shifted.

When wargame is not enough

Looking over history, little has changed in the wargaming besides the technology involved to present it. It still is a great tool to visualize battles and "close open flanks" in the planning. The relevance of the wargaming though, is often questioned outside the tactical level. The operational level campaign level wargaming for instance, needs strong "CONOPS (concept of operations) level" support from the tactical components in order to visualize battles. Therefore, the campaign wargaming would be held after the CONOPS development at the tactical level, which means the components need to be ahead of the joint level, although they start after this. In a realistic, time constraint planning environment, this comes with the cost of everybody doing their job before they are supposed to do it.

On another option, the campaign wargaming could hinge upon antagonizing the red and blue operational designs by applying a combination of belt and box methods to select the relevant opposing decisive conditions. In this case, most of the questions related to campaign wargaming are aimed at achieving or not the effects or decisive conditions built in the operational design. However, in order to answer these, the operational assessment needs to be a state-of-the-art product by that time, a goal usually much too high to be achieved that early in the planning.

Conclusion

A successful planning process is given not only by a good plan, but more importantly, by a thorough understanding of the situation, the problem set and the problem-solving methods. We listed here a few of the critical points in the planning process (commander's guidance, factor analysis, COG analysis, wargaming) where an unfitted approach can produce at least confusion and ambiguity. Ultimately, the planning community needs to come together, share and instill such remedies in the new COPD.

BIBLIOGRAPHY

1. COPD, *Comprehensive Operations Planning Directive v3.0*, October 2010;
2. JP 5-0, *Joint Planning*, June 2017;
3. JWP 5-00, *Joint Operations Planning*, June 2004;
4. Mason Carpenter, Talya Bauer, Berrin Erdogan, *Management principles,* 2012books.lardbucket.org, 2012;
5. Wood C. John, Wood C. Michael, *Henry Fayol Critical evaluations in business and management*, Routledge, London, 2002;
6. Navi Radjou, Jaideep Prabhu, Simone Ahuja, *Frugal Innovation: lessons from Carlos Ghosn, CEO, Renault Nissan*, hbr.org, 2012;
7. http://www.yourarticlelibrary.com/management/forecasting/forecasting-roles-steps-and-techniques-management-function/70032
8. https://mosaicprojects.com.au/WhitePapers/WP1094_Defining_Management.pdf

HUMANITARIAN INTERNATIONAL LAW

CHAIRS:

Mădălina-Daniela GHIBA, PhD
Daniela COMAN, PhD

REINTERPRETING THE CONCEPT OF *"JUS COGENS"* THE GENERAL PROHIBITION OF THE USE OF FORCE ANALYSED *VIA* THE REALPOLITIK APPROACH OF THE RUSSIAN FEDERATION

Lisa-Maria ACHIMESCU
Ph.D., National Defence University "Carol I"
lisa.achimescu@gmail.com

Teodor FRUNZETI
General (ret.) professor habil., Ph.D.,
"Titu Maiorescu" University
Academy of Romanian Scientists
tfrunzeti@gmail.com

Abstract: *More often than not the general principles guiding international law are interpreted and applied in a conceptual framework derived from and drenched in the constitutional traditions of European states. This approach has strengthened the liberal-oriented legal order, however, its' claim to universality remains void of factual support. Beyond the cultural boundaries of Europe, and beyond the institutional threshold of EU and the NATO, lay a differentiated approach, a realpolitik, profoundly pragmatic and state centric approach that has characterized the Russian Federation throughout history. The aim of our scientific endeavor is to analyse the prohibition of the use of force in reference to the Russian Federation in order to determine how the profoundly different behavior of an international state actor of such magnitude affects the international legal order.*

Keywords: *Russian Federation, jus cogens, legal order, realpolitik, international institutions.*

1. Prohibition of the use of force. Custom *versus jus cogens*

A priori, force and law are apparently irreconcilable concepts. The law prohibits the use of force and the international system of collective security is based on said prohibition, even if, in fact, armed conflicts remain an omnipresent reality of modern society. In reality, law and force are inseparable, given that upholding the law is not only ensured by coercion but also because the law constitutes, at least in part, a direct expression of a certain configuration in the equation of power relations. The "dangerous liaison" maintained between force and the law caught the attention of philosophers, from Aristotle[1] to Pascal[2], *via* Saint-Augustin[3] and Kant[4].

The principle of prohibition of the use of force represents one of the fundamental pillars in the collective security system established after the Second World War. Transgressed on different occasions, the question of its value is often debated and constantly evaluated. Indeed, some believe that the numerous impugnments on this principle have had the effect of altering its' value, making it fall into desuetude. This statement should be rejected because, if

[1] *See* Aristotle's major work "Politics", *introduction and translation* Jean Aubonnet, Paris, Les Belles Letttres, 1971.

[2] *See* Pascal's reference book "Pensées", 1671, posthumous, Brunschwicg (ed.), Paris, Hachette, 1897.

[3] *See* "The City of God", *in* "Works of Saint Augustine", 12 vol., Introduction and notes by G. Bardy, translation by Gustave Combès, Paris, Desclée de Brouwer, "Augustinian Library", 1975-1989.

[4] See Kant's very famous "Project of perpetual peace: A philosophical sketch"(Zum ewigen Frieden. Ein philosophischer Entwurf), text and translation by Jean Gibelin, Paris, Vrin, 1999.

the infringement of a rule of law obviously has consequences on its effectiveness, this cannot automatically call into question its very existence. Even if infringed, the principle of prohibition of the use of force remains a crucial norm of positive law.

After having remained a subject of academic discussions for a very long time, which was, furthermore, quite neglected, the concept of *jus cogens* acquired great topicality, since the International Law Commission referred to it in the draft articles on the law of treaties, elaborated in 1966.[5] The Commission's draft provoked a number of reactions on this particular point from state-actors, which were expressed, on the one hand, in the comments they submitted following the communication of the first text drawn up by the Commission and, on the other hand, by the statements made before the 6th Committee of the General Assembly, during the examination of the Report of the Commission.[6] The interest aroused by this initiative was also manifested in a whole series of doctrinal studies, as well as in the discussions pursued within the framework of scientific meetings.[7]

The debate concerned the strictly theoretical issues pertaining to the conditions which must be judiciously met for the emergence of *jus cogens* in a specific legal order. Specifically, it came into question whether or not *jus cogens* norms constituted a normative corollary already in place in the sacred pantheon of international law, emerged in a sense of *illo tempore,* only to be recognized, or if they can, in fact, be the result of normative evolution in an ever-changing society.

The concept of *jus cogens* has always had a relative character, due to the exceptions admitted by contemporary international law, such as individual and collective self-defence, the coercive action of the Security Council within the framework of Chapter VII of the UN Charter and, furthermore, the right of the peoples to self-determination. This relative nature was further accentuated by the terrorist attacks of September 11, 2001 and the US military operation against Iraq[8], which revealed that both the concept of self-defence and the role attributed to the Security Council in the field of collective security have been deeply redefined.

"All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[9] By thus prohibiting the threat of the use force and the use of force in international relations, Article 2(4) of the Charter of the United Nations alone constitutes a veritable revolution in the international legal order.[10] By putting an end to the recognition of a subjective right to war, it contributes to the abandonment of the classic *Westphalian* model.

[5] First draft articles on the Law of Treaties, art. 37 & 45. *See* Report of the International Law Commission, 1963, General Assembly Doc. of. IT session, supplement No. 9. The question had been discussed in the report by Sir Humphrey Waldock, A/CN.4/156, p. 51, who himself referred to the proposals of the two special rapporteurs who preceded him, Sir Hersch Lauterpacht and Sir Gerald Fitzmaurice; cf. Dehaussy, Yearbook, 1963, p. 600.

[6] *See* the text of these observations annexed to the Commission's 1966 report, cited above, p. 112 and *see also* the discussion on this topic at the "The 6th Committee of the General Assembly, during the 17th and 21st" sessions (cf. P. Raton, Yearbook, 1963, p. 562 and, 1966, p. 291).

[7] In particular the conference organized in Lagonissi (Greece) by the Carnegie Endowment for International Peace, in April 1966, whose work was the starting point for these reflections. The issue of *jus cogens* was introduced by a well-researched and comprehensive report by Profeessor E. Suy, *The concept of jus cogens in public international law.* The conference proceedings are currently published.

[8] The 2003 invasion of Iraq was the first stage of the Iraq War. The invasion phase began on 19 March 2003 (air) and 20 March 2003 (ground) and lasted just over one month, including 26 days of major combat operations.

[9] Art. 2 (4) of the United Charter; *Charter of the United Nations,* 24 October 1945, 1 UNTS XVI available at http:// www.refworld.org/docid/3ae6b3930.htlm, [accessed 20 February 2020].

[10] According to M. Viraly, Article 2 (4) constitutes "a real change in international law, a change which it is not excessive to qualify as revolutionary" *in* "Article 2 paragraph 4" in J.-P. Cot, A. Pellet (eds.), *The Charter of the United Nations. Article by article commentary*, Paris, Economica, 2nd ed., 1991, p. 115.

However revolutionary this provision may seem, before 1945, states had attempted to regulate the use of force. This was particularly the case during the two international peace conferences held in the Hague in 1899 and 1907.[11]

After the First World War, the question on the use of force, logically, gained renewed interest. Although the League of Nations Pact had attempted to impose *"the acceptance of obligations not to resort to war"*[12], it did not prohibit its use.[13] The Briand-Kellogg Pact of August 27, 1928 addressed this issue[14] by finally outlawing war and prohibiting the use of war as a means of national policy.[15] The pact *"constitutes the first denunciation of war by an international instrument of remarkable conciseness"*[16]. Its *Achilles' heel* resided, however, in the fact that the text did not stipulate any sanctions and, because of this legislative gap, the Briand-Kellogg Pact could not achieve its objective. Obviously, it did not prevent the Second World War and its endless procession of atrocities.

In the aftermath of the WWII tragedies, the world nations decided to create the normative framework that eliminated the possibility of making the use of war a discretionary, unilateral act. While article 2(4) of the UN Charter enshrines the prohibition of the use of force[17] as well as the threat of the use of force[18], the prohibition is not of absolute nature. Two issues should be addressed in this respect.

The first concerns the *scope of the norm*. The prohibition only applies in the context of international relations and only with regard to member states of the United Nations.[19] Furthermore, the use of force is prohibited only insofar as it is directed against the territorial integrity or independence of a state-actor or is undertaken in a manner incompatible with the purposes of the United Nations.

The second caveat that should be brought into focus relates to the exceptions allowing the use of force. On the one hand, the principle of the prohibition of the use of force cannot deprive state-actors of their essential right to defend themselves. Article 51 of the Charter of

[11] *See* Article 1 of the Convention for the Pacific Settlement of International Disputes adopted on July 29, 1899 in The Hague; *see also* Article 1 of the Convention (III) on the opening of hostilities adopted on October 18, 1907 in The Hague.

[12] Preamble of the League of Nations, Covenant of the League of Nations, 28 April 1919, available at: https://www.refworld.org/docid/3dd8b9854.html [accessed 29 February 2020].

[13] The Covenant prohibits wars of aggression (article 10), open conflict to contest an international judicial or arbitral decision (article 12 § 1) and war decided despite a recommendation adopted unanimously by the Council of the Council Chamber of the League of Nations. *See* Article 15 (4). In addition, before resorting to war, the States had first to submit their dispute to arbitration or to the Council Chamber of the League of Nations then respect a period of three months from the arbitral or judicial decision or the report of the Council. *See also* Article 12.

[14] *See* M.L.A., Miller, David Hunter, "*1875-1961. The Peace* Pact *of Paris; a Study of the Briand-Kellogg Treaty"*, New York; London: G. P. Putnam's & Sons, 1928.

[15] Article 1 of the Briand-Kellogg Pact: "The High Contracting Parties solemnly declare in the names of their respective peoples that they condemn recourse to war for the solution of international controversies, and renounce it, as an instrument of national policy in their relations with one another."

[16] N. Schrijver, *"Article 2, paragraph 4" in* J.-P. Cot, A. Pellet, M. Forteau (eds.), The Charter of the United Nations. Article by article commentary, Paris, Economica, 3rd ed., 2005, 2 vol., Vol. I, p. 437-467, p. 442.

[17] The term *"war"* has been abandoned in favor of that of *"use of force"*, as the second has a broader significance than the first. In addition, in order not to violate the Briand-Kellogg Pact, certain state-actors during the 1930s had resorted to the use of force, taking care not to qualify their action as an act of war. This is how Italy carried out an so-called *"expedition"* to Ethiopia while Japan called the invasion of Manchuria an *"incident"*. *See* N. Schrijver, "Article 2, paragraph 4", *op. cit.*, p. 442.

[18] As pointed out by the ICJ in the advisory opinion on the *Legality of the threat or use of nuclear weapons*, the concepts of "threat" and "use" of force go hand in hand: Advisory Opinion of 8 July 1996, Rec. ICJ, 1996, p. 246, para. 47.

[19] *n.n* Nowadays almost all states are members of the UN.

the United Nations recognizes state-actors' natural right to self-defence.[20] On the other hand, the Charter of the United Nations allows the Security Council to decide on coercive measures in the event of a *"threat to the peace, breach of the peace, or act of aggression"*[21]. Practice has since admitted that the Security Council can delegate its assigned power of constraint[22], issue that has been ardently debated in doctrine. It should be recalled that, pursuant to Article 43 of the Charter, the members of the United Nations have undertaken to negotiate agreements with the Security Council aimed, in particular, at making the armed forces available to the latter. Such agreements have never been adopted; this has inexorably made it necessary to delegate coercive power.

Thusly, the principle of prohibition of the use of force constitutes the core of the collective security system edifice established in 1945. Many resolutions of the United Nations General Assembly have recalled the existence of this principle[23] which, according to the International Court of Justice (ICJ)[24], constitutes the *"cornerstone of the Charter of the United Nations"*[25]. In 1986, the International Court of Justice even noted that it had acquired *customary value*.[26] The principle of the prohibition of the use force, therefore, has the dual *status* of a conventional and customary standard.

Last but not least, given its importance, this standard is often cited as an example of a *jus cogens* norm[27], in other words as an intransgressible principle, a norm unsusceptible of derogation. During the drafting of the Vienna Convention on the Law of Treaties, the principle of the prohibition of the use of force was presented by the International Law Commission which "*pointed out that the law of the Charter concerning the prohibition of the use of force in itself constitutes a conspicuous example of a rule in international law having the character of jus cogens*."[28]

The establishment of the prohibition on the use of force has not resulted in the cessation of all armed conflict, as, *per se*, this was not the main objective of state-actors in adopting Article 2(4). Indeed, the article does not concern internal conflicts and allows the use of force to be made lawful when intervening in the context of self-defence or when authorized by the Security Council. The problem however resides in the fact that, as of late, there has been use of force in international relations without either of these two conditions being met. Currently, international law norm infringements are increasing. The war of good *versus* evil leads to a

[20] The question of the existence of a standard enshrining the principle of self-defense did not logically arise as long as the resort to war was a discretionary act. It was the consecration of the principle of the prohibition of the use of force that led to questions about the existence of a principle of self-defense. *See* A. Cassese, *"Article 51"*, *in* J.-P. Cot, A. Pellet, M. Forteau (eds.), The Charter of the United Nations. Article by article commentary, Paris, Economica, 3rd ed., 2005, 2 vol., Vol. I, pp. 1329-1362.

[21] According to the structure of the Charter of the United Nations, the Security Council must first qualify the situation (Article 39) and then take action. These can be provisional (Article 40) and imply force (Article 42) or not imply it (Article 41).

[22] V. N. Blokker, *"Is the Authorization Authorized? Powers and Practice of the UN Security Council to Authorize the Use of Force by "Coalitions of the Able and Willing"*, European Journal of International Law, vol. 3/11, 2000, pp. 541-568.

[23] The principle of the prohibition of the use of force has been reaffirmed by a number of resolutions of the United Nations General Assembly. *See for example* the following resolutions: 2625 (XXV) of October 24, 1970, 2660 (XXV) of December 7, 1970, 3314 (XXIX) of December 14, 1974, A/RES/31/9 of November 8, 1976, A/ RES/33/72 of December 14, 1978, A/RES/42/22 of November 18, 1987.

[24] International Court of Justice herein after *"ICJ"*.

[25] ICJ, *Armed activities in the territory of the Congo* (Democratic Republic of the Congo v. Uganda), judgment of 19 December 2005, para. 148.

[26] ICJ, *Military and paramilitary activities in and against Nicaragua* (Nicaragua v. United States of America), Rec. ICJ, 1986, p. 103, para. 193.

[27] Yearbook of the International Law Commission, Volume II, p. 247.

[28] *Ibidem.*

reminiscence of the previous messianic conception of *just war*.[29] These numerous and frequent violations have led some authors to assert that the norm prohibiting the use of force has either evolved into a *summa exceptio* or no longer exists.[30] It is the assertion of certain specialists and reputed authors that the prohibition of the use of force has fallen into disuse or even disgrace.[31] The doctrine which transforms and reinterprets aggression in the matrix of the law tends to justify the return to *unilateralism*[32]; it represents an attempt to iron out all, if any, "flaws" of the United Nations Charter system, in which the use of force can only be collective, apart from the exercise of the right to self-defence.

In nuce, the prohibition of the use of force represents a sort of *Copernican revolution*[33] in law and a primordial principle of the United Nations system because, according to the Preamble of its' Charter, this organization was created to "*save succeeding generations from the scourge of war"* and aims to *"maintain international peace and security"*[34].

Because of its conventional and customary value, and its recurrent application both by UN bodies and by state-actors, the principle of prohibition of the use of force is considered to be a *jus cogens* norm, that is to say, according to article 53 of the 1969 Vienna Convention "a peremptory norm of general international law is a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character"[35].

[29] The authorship of the *just war theory* goes mainly to Christian theologians who had wondered how to reconcile the use of force and their faith.

[30] Th. Franck was the first to announce the evolution of the content of Article 2 (4) *in* "Who Killed Art. 2 (4)? or: Changing Norms Governing the Use of Force by States", American Journal of International Law , 1970, vol. 64/4, p. 809-837. Since then, others have followed him: E. Rostow, "The Legality of the International Use of Force by and from States", Yale Journal of International Law, 1985, vol. 10, p. 286-290; J. Bolton, "Is there really "law" in international affairs", Transnational Law and Contemporary Problems, 2000, vol. 10/1, pp. 1-48; A. C. Arend, "International Law and the Preemptive Use of Force", The Washington Quarterly, 2003, vol.26/2, pp. 89-103.

[31] M. Glennon, "How International Rules Die?", The Georgetown Law J.ournal, 2005, vol. 93/3, p. 939-991. *See also by the same author*: "Limits of Law, Prerogatives of Power. Interventionism after Kosovo", New York, Palgrave, 2001, pp. 60-64 & p. 84; "The Fog of Law: Self-Defense, Inherence, and Incoherence in the United Nations Charter", Harvard Journal of Law and Public Policy, 2002, vol. 25/2, pp. 539-558; "Why the Security Council Failed", Foreign Affairs, 2003, vol. 82/3, pp. 16-35; "The Rise and Fall of the UN Charter's Use of Force Rules", Hastings International and Comparative Law Review, 2004, vol. 27/3, pp. 497-510; "The Emerging Use of Force Paradigm", Journal of Conflict & Security Law, 2006, vol. 3/11, pp. 309-317.

[32] Oscar Schachter in his paper "The Lawful Resort to Unilateral Use of Force" considers that: "A state may lawfully resort to unilateral use of force outside of its territory in the following circumstances:' 1) When it has been subjected to an armed attack on its territory, vessels or military forces; 2) When the imminence of an attack is so clear and the danger so great that the necessity of self-defense "is instant (and) overwhelming"; 3) When another state that has been subjected to an unlawful armed attack by a third state requests armed assistance in repelling that attack; 4) When a third state has unlawfully intervened with armed force on one side of an internal conflict and the other side has requested counter intervention in response to the illegal intervention; or 5) When its nationals in a foreign country are in imminent peril of death or grave injury and the territorial sovereign is unable or unwilling to protect them."

[33] We use the term "Copernican revolution" in the same way as the analogy used by Kant. As Copernicus discovered that the earth revolves around the sun, while the opposite was thought before him, similarly, in *The Critique of Pure Reason,* Kant reverses the traditional relation *subject v. object,* the subject becoming central to knowledge.

[34] Preamble of the *Charter of the United Nations,* 24 October 1945, 1 UNTS XVI available at http:// www.refworld.org/docid/3ae6b3930.htlm

[35] Article 53 of the *Vienna Convention on the Law of Treaties*, 23 May 1969, United Nations, Treaty Series, vol. 1155, p. 331, available at: https://www.refworld.org/docid/3ae6b3a10.html [accessed 28 February 2020]

2. The Russian Federations' approach to international law

Following the dissolution of the Soviet Union, Russia found itself faced with the imperative to formulate its own foreign policy, based on both its strengths and aspirations. While the states' capabilities are still enormous, aspirations have undergone significant changes since the fall of the Communist bloc. It should be noted that Russia has not only preserved its membership in international organizations, but has also considerably extended its presence on the international scene. As a member of the UN Security Council, replacing the USSR as a successor state, it also became a member of the Council of Europe and the World Trade Organization; in 2013, the Russian Federation assumed the presidency of the G20 and, in 2014, that of the G8, but, alas, in 2017 announced its permanent withdrawal from the G8. Since 2014, following the Ukrainian crisis and the Crimean annexation, Russia focused mainly on its participation at the G20 Forum.

Russian doctrinarians brush aside the idea that Russia would reject the western approach to international law, supporting their thesis on the fact that since the dismantling of the USSR Russia has ratified a large number of international treaties, such as the Law of the Sea Convention, in 1997 and has acceded to the European Convention on Human Rights, in 1998. Likewise, while the USSR was of dualist tradition[36], the 1993 Constitution adopted a monistic vision[37], thus going in favor of strengthening the implementation of international law standards in Russia, even if this needs to be qualified in practice, as highlighted by cases concerning the application of the European Court of Human Rights' (ECtHR) [38] judgments, a representative exemplification being the *Yukos case*[39]. Thus, in its recent history, Russia has operated a veritable legal revolution by adhering to the general principles of general international law, overwhelmingly rejected by the dominant Soviet opinion.

While Russia's foreign policy is frequently criticized, the study of Russian doctrine in international law continues to be often enough overlooked. Surprisingly, Russian jurists are well acquainted with "western" approaches to international law, while the reverse is often less true. Russia's attachment to the concept of state sovereignty constitutes a common thread in the Russian approach to international law that constitutes the coalescence between Soviet ideology and adherence to the fundamental principles of international law.

According to Russian "official" perception, the new world order must constitute a stable system of international relations, based on the principles of equal rights, reciprocal respect and mutually advantageous cooperation of state-actors, in accordance with international law.[40] The United Nations must remain at the crux of international relations regulation and coordinate global policy in the 21st century, as it has proven its essential character and unique international legitimacy. Thus, Russia affirms to support the efforts to strengthen UNs' essential coordinating role.[41] This implies, in particular, unconditional respect for the objectives and principles set out in the Charter of the United Nations and the implementation

[36] Dualism in constitutional tradition considers that the international legal system is normatively distinct from the realm of domestic law.

[37] The monistic vision in constitutional law affirms that a rule of international law need not be incorporated into the domestic legal system to become legally relevant, as it has binding value upon its institutions and subjects.

[38] European Court of Human Rights hereinafter "ECtHR".

[39] On July 31, 2014, the European Court of Human Rights (ECtHR) in Strasbourg announced its largest ever award of Just Satisfaction. The award of €1.9 billion ($2.5 billion) to Yukos Oil Company (Yukos) is 21 times larger than any previous award made by the ECtHR in its history. "Yukos was the object of a series of politically motivated attacks by the Russian authorities that eventually led to its destruction," the arbitration panel found, adding that Moscow had aimed to "bankrupt Yukos, assign its assets to a state-controlled company and incarcerate Mr Khodorkovsky who gave signs of becoming a political competitor" to Russian president Vladimir Putin.

[40] Rustam Ksyanov, "*The Russian Approach to International Law and European Integration", French Yearbook of International Relations, 2013, p. 526.

[41] *Ibidem.*

of rational reforms of the United Nations, in order to gradually adapt to the ever-changing political and economic realities of the world; the Russian position is that any decision to additionally augment the number of members of the UN Security Council must be taken on the basis of the broadest consent of the member states of the UN.[42]

As claimed by Russian doctrinarians, international security largely depends on Russia's compliance with its international obligations under international treaties relating to the non-proliferation of weapons of mass destruction, arms control and disarmament.[43] They insists on the obligation to respect these international commitments and, in this spirit, Russia has to prove its willingness to conduct talks with the other nuclear powers in order to reduce strategic offensive weapons to a level sufficient enough to maintain strategic stability.[44]

As stated by the former judge of the European Court of Human Rights, A.I. Kovler, who analyzed the Russian Constitution in relation to European human rights law, Article 15(4) and Article 17(1) of the Russian Constitution are pursuant to the provisions of the Council of Europe Statute, as well as with the provisions of the European Convention on Human Rights, more particularly its Preamble and Article 1, which enshrines the "*obligation to respect human rights". In examining article 46(3) of the Constitution, A.I. Kovler emphasizes that "the universalization of the legal status of an individual, the assumption by an individual of international legal personality, finds adequate reflection in an expansion of possibilities of the individual's international-legal protection (...) This standard is in compliance with the Article 34 of the Convention, "Individual applications""*[45]. The author further notes that Russia, having signed and ratified the ECHR[46], has thereby recognized, according to Article 46 of the Convention, "*the jurisdiction of the European Court of Human Rights and the binding nature of its decisions. At a practical level, this means that the Russian Federation, as a respondent State and, in the event of recognition by the Court of the violation of one of the rights of the applicant which is recognized by the Convention, is compelled to adopt measures of an individual character (e.g. restitution in integrum), as well as general measures (for example, revision of certain provisions of domestic law, implementation of special legislative measures etc.) "*[47].

In general, it should be noted that, in Russian doctrine, more and more attention is paid to the question of the relationship between the norms of international law and those of domestic law. Thus, S. J. Marochkin believes that *"universally accepted norms of international law take precedence over Russians laws"*[48]. Furthermore, universally accepted principles of international law have primacy in the Russian legal system over the norms of national law, including those of a constitutional nature.[49] The position of the Constitutional Court, expressed in the opinion of Judge O. I. Tiunov, is characteristic in this respect: *"the Court considers that the universally accepted principles and norms of international law, as well as Russia's international agreements, take precedence over internal laws in the event of a contradiction between international legal norms and domestic legislation"*[50]. I. I. Lukashuk has awarded an even higher level to universally accepted human rights principles and

[42] *Ibid.*, pp. 527-546.

[43] *Ibidem.*

[44] *Ibidem.*

[45] A. Kovler, "*The Individual as a Subject of International Law (Discussion Revisited)"*, Doctor of Legal Sciences, Professor, Judge of the European Court of Human Rights, Ukraine Law journal, no. 2, 2013, p. 32.

[46] European Convention on Human rights hereinafter "ECHR".

[47] *Ibid.*, pp. 39-40.

[48] S. J. Marochkin, "International Law in the Russian Courts in Transitional Situations", *in* E. Kristjansdottir, A. Nollkaemper and C. Ryngaert (eds.), International Law in Domestic Courts: Rule of Law Reform in Post-Conflict States (Intersentia: Cambridge–Antwerp-Portland, 2012), p. 37.

[49] *Ibidem.*

[50] O. I. Tiunov, *"Constitutional Court of the Russian Federation and International Law", PEMII*, 2006, p. 180

standards: "*We can speak with certainty of the primacy of universally accepted human rights standards in the Russian legal system*"[51]. These examples attempt to illustrate, that, at least, at a theoretical level, there is a clear tendency in the Russian legal system to recognize the pre-eminent position of international law over the national legal system.

It remains to be seen whether the Russian normative basis follows the same international legal trend and what are the main gaps of the legal system that still remain unresolved, problematic or thorny. At present, it would not be unreasonable to say that within the Russian legal system the understanding of human rights has deepened considerably under the influence of the ECHR and other European instruments. Most European standards and principles in this area have found their right place in Russian law. Since 1992, Russia has actively participated in intergovernmental human rights and legal reform programs. Long before the official entry into the Council of Europe, Russia adopted a series of federal laws which reflect its will to reform the legal system.[52] What happened during 1993 represent a very significant moment from this point of view; apart from the new Russian Constitution, several federal laws have emerged. Thus Russian doctrinarians consider that we are witnessing the strengthening of judicial protection of the rights and freedoms of Russian citizens;[53] Russians are granted additional possibilities with regard to freedom of movement and residence on Russian soil[54] and the rights of refugees are also confirmed and clarified[55].

After the entry into force of the new Russian Constitution, certain standards of the ECHR and other Council of Europe conventions were incorporated into several federal laws adopted by the Federal Assembly of Russia. Thus, the federal law relating to the Constitutional Court of the Russian Federation (1994)[56], the federal law on the detention of persons suspected or accused of the commission of crimes (1995)[57] and other legislative acts have provided additional guarantees of rights and freedoms deemed inherent in any democratic society: the right to life, the right not to be tortured or to undergo inhuman or degrading treatment or punishment, the right to liberty and personal inviolability, the right to effective protection provided by the judicial system.

Upon joining the Council of Europe, Russia pursued to make over thirty changes to its legislative base. Among other things, it undertook to adopt a law establishing the *Ombudsman institution* in Russia; the need for this institution emerged in the early 1990s, when Russian society embarked on the path of democratic reform. The institution of the Ombudsman was finally provided for in the Russian Constitution (Article 103(1)).[58] Following the accession to the Council of Europe, Russia undertook to sign and ratify the ECHR's Protocol No. 6, concerning the abolition of the death penalty. In the meantime, the Russian government has been required to establish a moratorium on the death penalty.[59] However, the agreed upon obligations were not respected. In its resolution of the 29th of January 1997, the Parliamentary Assembly of the Council of Europe pointed out the fact that, while death sentences have no

[51] I. I., Lukashuk, *"The Principle Pacta Sunt Servanda and the Nature of Obligation Under International Law",* The American Journal of International Law, no. 3, 1997, pp. 513-18. Accessed March 1, 2020. doi:10.2307/2203309.

[52] Rustam Ksyanov, *op. cit.*, p. 541.

[53] Law on "Recourse to justice against acts and decisions violating the rights and freedoms of citizens", April 27, 1993.

[54] Law on "the right of citizens of the Russian Federation to move and freely choose their place of residence in the Russian Federation ", 25 June 1993.

[55] "Refugee Status" Act, 19 February 1993.

[56] Federal Law on "The Constitutional Court of the Russian Federation", July 21, 1994.

[57] Federal Law on "The Detention of Persons Suspected or Accused of a Crime", 15 Jul 1995.

[58] *See* the Constitution of the Russian Federation, 12 December 1993.

[59] Parliamentary Assembly Opinion No. 193 on Russia's application for membership of the Council of Europe, doc. 7 443, Report of the Political Affairs Committee (rapporteur Mr. Muehlemann), and doc. 7,463, Opinion of the Committee on Legal Affairs and Human Rights (rapporteur Mr. Bindig).

longer been carried out in Russia since the 4th of August 1996, the issue must remain a central point of focus for the Russian government.

Indeed, Russia has not fulfilled its obligations in this area because it has not officially declared the introduction of the moratorium on the death penalty which was to result in the adoption of a corresponding law.[60] Currently, the death penalty is no longer imposed in Russia, as on November 19, 2009, the Constitutional Court of the Russian Federation spoke in favor of extending the moratorium on the death penalty. Moreover, the decision to definitively abolish the death penalty ultimately fell in *Duma's* purview, which had to pass a law to that effect, although certain deputies were not in favor of adopting such a provision.

With regard to Russian case law and general practice pertaining to fundamental rights, it should be noted that European standards are becoming more and more established in the Russian legal system thanks to the judgments delivered by the various European judicial bodies. The example of the Russian Constitutional Court is quite eloquent: over a period of a few years, the Constitutional Court has adopted around twenty decrees which refer directly to the case law of the European Court of Human Rights, thus drawing the attention of the Russian legislator to the non-conformity of several Russian laws not only with the Constitution, but also and above all with the ECHR and the European case law, and, with the European *acquis* of the jurisprudence on the matter. This constitutes a fairly significant result, especially if one takes into account that the Constitutional Court is considered one of the supreme judicial authorities of the Federation[61].

Furthermore pertaining to Russian cases, it should be observed that the European Court of Human Rights, finding infringements of the ECHR's various articles and Protocols (*for instance*: Articles 2[62], 3[63], 5, 5(1), 5(3), 5(4)[64], 6(1)[65], 8[66], 10[67], 11[68], 13[69] and 18[70], as well as Protocol 1(1)[71]), presents itself as a judicial mechanism enabling Russian citizens to deal with the shortcomings of their own national legal system.

From a substantive point of view violations of Article 3 (Prohibition of torture), Article 5 (Right to liberty and security), Article 6 (Right to a fair trial) of the ECHR, as well as of Article 1 of Protocol No. 1 of the ECHR (the enforcement procedure and its duration[72]) which are regularly under scrutiny in the jurisprudence of the Strasbourg Court.

[60] Parliamentary Assembly Resolution No. 1,111 on honoring the commitment entered into by Russia when it joined the Council of Europe to establish a moratorium on capital executions, text adopted by the Assembly on 29 January 1997 (5th meeting). *See also* Mrs. Wohlwend, Report of the Committee on Legal Affairs and Human Rights, doc. 7,746, Council of Europe Parliamentary Assembly, 2007.

[61] Article 125 of the Russian Constitution.

[62] *Troubnikov v. Russia*, req. 49 790/99, Council of Europe: European Court of Human Rights, 5 Jul 2005.

[63] *Kalashnikov v. Russia*, req. 47 095/99, Council of Europe: European Court of Human Rights, 15Jul, 2002.

[64] *Smirnova v. Russia*, req. 46 133/99 and 48 183/99, Council of Europe: European Court of Human Rights, Jul 24, 2003.

[65] *Burdov v. Russia*, req. 59 498/00, Council of Europe: European Court of Human Rights, 7 May 2002.

[66] *Znamenskaya v. Russia*, req. 77 785/01, Council of Europe: European Court of Human Rights, June 2, 2005.

[67] *Grinberg v. Russia*, req. 23472/03, Council of Europe: European Court of Human Rights, 21 Oct, 2005.

[68] *Presidential Party of Mordovia v. Russia*, req. 65 659/01, Council of Europe: European Court of Human Rights, Oct 5, 2004.

[69] *Kuzine v. Russia*, req. 22 118/02 and *Klyakhin v. Russia*, req. 46 082/99, Council of Europe: European Court of Human Rights.

[70] *Garabayev v. Russia*, 38411/02, Council of Europe: European Court of Human Rights, 7 June 2007.

[71] *Sukhoruktchenko v. Russia*, req. 69 315/01, Council of Europe: European Court of Human Rights, 10 Feb 2005.

[72] Guide on Article 1 of Protocol No. 1 to the European Convention on Human Rights - para. 171: "States are under a positive obligation to organize a system for enforcement of judgments that is effective both in law and in practice and ensure that the procedures enshrined in the legislation for the enforcement of final judgments are complied with without undue delay (*see* Fuklev v. Ukraine, para. 91)."; para. 172: "(…)the extent of the State's obligations under Article 1 of Protocol No. 1 varies depending on whether the debtor is the State or a private

In regard to the Russian cases, a detailed analysis of the case-law, leads to the formal review of these judgments, but it does not entitle us to have a say on certain particularities in the approach of the Strasbourg Court while examining East European litigation. Indeed, fears related to the initiation, in the activity of the European Court of Human Rights, of the so-called "double standards" policy *vis-à-vis* the new members has not materialized. *"At the risk of disappointing, rightly points out Florence Benoît-Rohmer*[73]*, it must be noted that, as a whole, the litigation before the European Court of Human Rights of the new States Parties to the Convention hardly differs from that of Western democracies, if not by a few peculiarities linked to the political and historical circumstances which surrounded their democratic transition. In addition, the Court has evidently taken care not to apply different standards to newly accessed states. The risk of a two-speed Europe concerning freedoms and rights seems therefore, for the moment at least, to have been ruled out."*[74]

Another important decision imposed by the ECtHR on Russia was in the case *Georgia v. Russia*[75] when the Court (ECtHR) applied a fine of 10 million Euros on Russia for having expelled Georgian citizens from its territory. According to a statement issued by the Strasbourg Court, Russia collectively expelled 1,500 Georgian nationals from its territory in 2006, imposing on them *"a coordinated policy of arrest, detention and expulsion*".

The European Court of Human Rights has declared admissible the application lodged by Georgia against Russia, *"in the context of the armed conflict that occurred between Georgia and the Russian Federation in August 2008 following an extended period of ever-mounting tensions, provocations and incidents that opposed the two countries"*[76], concerning the claims of violations of the European Convention on Human Rights which were allegedly committed by the defendant during the conflict between these two States parties to the Convention[77] during the month of August 2008. This judgment takes the opposite view from the position of the International Court of Justice in a dispute between two belligerent state-actors. Russia claimed that its August 2008 intervention in the Georgian region of South Ossetia was nothing more than self-defence, in order to protect its citizens.

ICJ applied the proportionality criterion in similar cases like Nicaragua[78] and Nuclear Weapons[79], not without foundation: the Court made the connection between the proportionality criterion and the necessity to curtail an attack. Notwithstanding, the ICJ's opinion on the application of the proportionality criterion is as veiled as it is the analysis of the intricate relationship between the scale of an attack, the proportionality of the response

person (*see* Anokhin v. Russia (dec.) & Liseytseva and Maslov v. Russia, para. 183); para. 173: "When it is the State which is the debtor, the Court's case-law usually insists on the State complying with the respective court decision both fully and timeously (Anokhin v. Russia (dec.); Burdov v. Russia, §§ 33-42). The burden to ensure compliance with a judgment against the State lies primarily with the State authorities starting from the date on which the judgment becomes binding and enforceable (*see* Burdov v. Russia (case no. 2), para. 69)," etc.

[73] Florence Benoît-Rohmer is a French jurist, specializing in European Law and Human Rights, and currently a Professor of Public Law at the University of Strasbourg.

[74] Florence Benoît-Rohmer, *"Le particularisme du contentieux concernant les pays d'Europe central et orientale"*, L'Europe des libertés, no. 9, 2002, p. 8.

[75]Case *Georgia v. Russia* (I), Application no. 13255/07, (just satisfaction), ECLI:CE:ECHR:2019:031JUD001325507, Council of Europe Of Human Rights, ECHR, 31 January 2019.

[76] *Ibid.*, para. 18.

[77] Georgia has been a party to the European Convention on Human Rights since April 27, 1999; Russia has been since February 28, 1996.

[78] ICJ (1986), Judgment on the case concerning *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America), 27 June, http://www.icj cij.org/docket/index.php?case=70.

[79] *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, I.C.J. Reports 1996, p. 226, International Court of Justice (ICJ), 8 July 1996, available at: https://www. refworld.org/cases,ICJ,4b2913d62.html [accessed 1 March 2020]

and the attempt in subsiding the attack; all the afore mentioned issues are not explored in detail in ICJ's jurisprudence.

In support of its request, Georgia claims various violations of the European Convention on Human Rights allegedly committed by the Russian armed forces and the Ossetian and Abkhaz insurgent forces placed under Russian effective control against the civilian population Georgian. Georgia based its allegations on the indiscriminate and disproportionate attacks allegedly carried out by the Russian forces, and by the separatist forces acting under their control, and on the lack of investigation which should have resulted therefore. According to the Georgian state, the acts carried out by Russia would have resulted in the creation of an administrative practice violating the rights guaranteed by the Convention; a practice allegedly perpetrated independently of the interim measures issued by the Court[80] pursuant to Article 39 of the Convention.

Russia, for its part, considers these allegations unfounded and based on a distortion of the facts. According to Russia's opinion, the use of force constitutes part of an act of self-defence aimed at defending the civilian population against the Georgian offensives.

Indeed, Russia invoked, in support of its first preliminary objection, that the violations alleged by Georgia did not fall within the jurisdiction of the Court because the European Convention on Human Rights limits the jurisdiction of a state to the principle of territoriality. Under this principle, the Court should only deal with alleged violations if they are committed within the territory of the state for which responsibility is invoked or in areas outside the national territory if the state exercises effective control over them.

In response to this argument, the Court invokes its jurisdiction to examine on a preliminary basis the dispute, as it falls within its jurisdiction pursuant to the principle *rationae loci*. Indeed, the question of whether the acts presented before the Court depend on the jurisdiction of the Russian state requires a decision regarding the qualification to be given to the acts committed by Russia outside its territory and to the nature of the possible control exercised over the areas in which the alleged acts occurred. This position raised doubts that the Strasbourg judges had been addressing before in *Bankovic v. Belgium et al.* [81] (December 12, 2001); the case debated whether the applicants fell within the jurisdiction of the respondent states within the provisions of Article 1 of the Convention. In this case the Court had adopted a restrictive, mainly territorial, concept of jurisdiction, by ruling that it had jurisdiction to hear cases concerning military operations carried out abroad, outside of the effective control of *"military occupation or in by consent, invitation or acquiescence of local government"*[82]. The Court therefore returns to a more classic posture in order to establish its jurisdiction, without requiring either occupation or consent, which seems to mark its desire to continue investigating the case on its merits.

The last objection of inadmissibility raised by Russia was based on the condition of exhaustion of domestic remedies.[83] The defendant alleges that the plaintiff has not complied

[80] EDH Court, Communiqué from the Registrar of August 12, 2008: "On August 12, 2008, the President of the Court, acting as President of the Chamber, decided to apply Article 39 of the Rules of Court (interim measures), considering that the current situation carries a real and continuous risk of serious violations of the Convention. In order to prevent such violations, the President, applying Article 39 of the Rules of Court, calls on the two High Contracting Parties concerned to honor the commitments entered into by them under the Convention, in particular with regard to Articles 2 and 3 of the Convention. (…)."

[81] *Banković et al v. Belgium et al*, Admissibility, App no 52207/99, ECHR 2001-XII, [2001] ECHR 890, (2007) 44 EHRR SE5, 11 BHRC 435, (2001) 123 ILR 94, IHRL 3273 (ECHR 2001), 12th December 2001, European Court of Human Rights [ECHR]; Grand Chamber [ECHR]

[82] EHR Court, Grand Chamber, December 12, 2001, *Bankovic v. Belgium et al.*, Application No. 52207/99, para. 59-73.

[83] European Convention on Human Rights, Article 35(1): "The Court may only deal with the matter after all domestic remedies have been exhausted, according to the generally recognized rules of international law, and within a period of six months from the date on which the final decision was taken."

with this condition, and that the latter is applicable in the present case because the proof of an administrative practice, which alone makes it possible to exclude it, has not been made. The Court dismissed this objection, considering that the proof of the existence of an administrative practice cannot be made at the stage of examining the admissibility of the application and that consequently the exception must be joined to the case's merits.[84] It finally recognized that the six month period provided for in Article 35(1) was respected.

In the concert of the requests introduced by Georgia[85] and in reaction to the facts which took place during the conflict of August 2008, the European Court of Human Rights asserts itself as being the first international court able to provide a jurisdictional response to the acts committed.

Other noteworthy cases presented before the ECtHR are *Issayeva*, *Youssoupova and Bazaïeva v. Russian,*[86] judgment that addressed, from a strictly legal point of view, the confrontations that took place between the Russian governmental forces and the Chechen rebel forces, in Grozny 1999 and *Issayeva v. Russia*[87], a case brought in front of the Court by Zara Issayeva who lost her son and three nieces in aerial bombardment and artillery fire by the Russian army on the village of Katyr-Yourt.

In the first case, on October 29, 1999, while residents of Grozny were trying to flee the fighting in the capital, the Russian army bombarded a convoy of civilians. As a result of the aerial bombardment, Medka Issayeva was injured and her two children and her daughter-in-law were killed; Zina Youssoupova was injured by shrapnel in the neck, arm and hip; the car belonging to Libkan Bazaïeva and containing his family's property was destroyed. The European Court found that Russia was responsible for the deaths and the violation of Ms. Bazayeva's right to peaceful enjoyment of her possessions.

In the second case, *Issayeva v. Russia*, although Russian forces had declared the village a "safe area" for those fleeing the fighting that was taking place in other parts of Chechnya, the European Court found that two senior army officers, General Major Yakov Nedobitko and General Major Vladimir Shamanov were responsible for the operation, during which was made massive use of "*indiscriminate weapons*"[88], causing the loss of civilian lives. The Court did not analyze whether it was dealing or not with a conflict, and, based its judgment only on the merits of the Convention's provisions, without resorting to international humanitarian law (IHL)[89]. One of the consequences of the Court's approach was the fact that only used in its consideration on the case the norms that generate obligations for the government, in direct correlation to human rights violations and not for the other parties involved, in accordance to the provisions of the international humanitarian law.

In this case the European Court has established that the Russian security forces have committed serious human rights infringements in Chechnya, including murders, enforced disappearances, acts of torture, unlawful destruction of property, as well as breaches of privacy during of illegal searches. The Court considered that Russian officials were negligent in their investigations into complaints by victims of abuses perpetrated by Russian soldiers.

[84] Commented judgment, para. 90 and 94.

[85] To the referral to the EHR Court and the ICJ, we must also add that of the ICC (*Cf.* report of the International Criminal Court, September 17, 2009, document N.U. A / 64/356).

[86] *Issayeva c. Russie; Youssoupova c. Russie; Bazaïeva c. Russie*, 57947/00; 57948/00; 57949/00, Council of Europe: European Court of Human Rights, 24 February 2005, available at: https://www.refworld.org/cases,ECHR,422341924.html [accessed 1 March 2020]

[87] *Issayeva v. Russia*, 57950/00, Council of Europe: European Court of Human Rights, 24 February 2005, available at: https://www.refworld.org/cases,ECHR,4223422f6.html; Accessed 7/05/2019.

[88] An indiscriminate weapon is a weapon that cannot be directed at a military objective or whose effects cannot be limited as required by international humanitarian law (IHL). Under IHL, the use of such an "inherently" indiscriminate weapon is prohibited.

[89] International Humanitarian Law hereinafter "IHL".

Authorities failed to immediately open investigations or take basic investigative steps, including interviewing witnesses or potential perpetrators identified in video footage or other material. The indifference displayed by the Russian government, as illustrated by aborted investigations, caused serious suffering that met the threshold of inhuman treatments towards the relatives of the victims. The European Court found that Russia has failed to offer victims the opportunity to obtain justice in Russia. Due to incomplete and inappropriate investigations, no perpetrators have been identified; in the absence of suspects, no case has ever been brought to justice. The Court found that the Russian authorities had breached their obligation to cooperate by refusing to present the required documents. The Russian authorities have repeatedly rejected requests from the European Court to obtain documents in the files concerning Chechnya, claiming that national law prevented them, either because investigations were under way or because the documents contained state secrets.

Unfortunately, the international community has failed to protect the Chechen population from widespread human rights violations. Governments and international organizations have refused to follow up on their statements of concern with measures that have political, financial or other consequences for Russia. The recent European Court judgments on Chechnya provide an objective assessment of Russia's responsibility for human rights infringements. They constitute an opportunity for the international community, and in particular for the member states of the Council of Europe, to persuade the Russian government to put an end, once and for all, to the general violations of human rights in Chechnya and to demand accountability from the perpetrators of these acts.

The ECtHR sets legal standards in the field of fundamental rights which are common to the different European states. The Convention can be objectively recognized as one of the most successful international agreements in the field of the protection of human rights. The assertion of the European legal space in post-Soviet countries still poses several problems.

The example of the Russian Federation constitutes clear proof in this respect. The pursuit of reforms and the correction of those already underway constitute the necessary conditions before one can address the effective integration of Russia into the European legal area in the domain of fundamental rights. A special role in this process belongs to Russia's judicial bodies, as well as to the European Court of Human Rights.

3. Realpolitik approaches to changing the status quo: Russia's return to internationally accepted behaviour

The global scene has remained, as it has always been, chaotic, fragmented and viscous, comprised of a plethora of antagonisms and always prone to dissension. The compelling information on the return to *realism* bestows the theory and practice of *Realpolitik* or *power politics* its rightful place in the international debate. Indeed, the EU's adoption of the idealist, neo-Kantian and functionalist conception of sovereignty emphasized its inner architectural construction, and therefore the "veiled" notion of governance. This debate put forward the concept of civil society, and therefore the subjective sense of citizens advocating the indefinite extension of freedom and rights, unbalanced by obligations and duties. The *"affectio societatis"*[90] prevailed over *"civitatis ac autoritatis"*[91], further depoliticizing the *"agora"*.

The real *ratio errorem* (n.n system error) resides in the analysis of Europe's place in the international hierarchy and in the distribution of global power, and, by comparison, Russia's position, which pushes to reorient the Union's concerns towards the international

[90] *Affectio societatis* is the Latin expression meaning that two people wish to enter into a partnership. It is, to be accurate, the "animus" (a word that is frequently used in jurisprudence, *the mind*, in the meaning of *intention*) to constitute a society.

[91] Latin for *"the city and its authority"*.

scene and its evolution. Thus, the return of *Realpolitik* becomes the bearer of a new culture in the international system and of a politico-strategic revolution, which no multilateral or legal reading could have brought to the understanding of the international arena, by any standards, be they supranational or transnational, nor to the government of "civil societies" by means of the norms of law. In the present international climate the United Nations, for various reasons, too many and complicated to discuss here, is unable to take on the role of supreme international arbiter on its own. *Exempli gratia*, the ascendancy taken by Pope Francis over António Guterres as the first moral figure on the planet illustrates the shortcomings of the venerable institution. China, too absorbed by its own "weight", is not ready to assume this role and Putin's Russia has no legitimacy to do so. The "emerging" countries, beyond the ranting, seem still far from being able to assume such responsibilities on a world level. There remains Europe, which is a bit like an elephant in a china shop, overwhelmed by the implications of assuming such an immense role.

According to political science professor Frédéric Charillon, the Ukrainian crisis *"confirms (...) the end of a European illusion according to which old-style conflicts (invasion of one state by another) would be definitively excluded in the strategic neighborhood of the European Union"*[92]. For any researcher, one of the crucial questions is whether this crisis represents "the typical symptom of a *Realpolitik* practice illustrating a perfectly mastered chess player strategy (*n.n* on the part of Vladimir Putin), or *vice versa*, a loss of control linked to an authoritarian drift"[93]. He added that "for Putin, the consequences of losing the base (n.n his political base[94]) far outweigh the effects of sanctions and political affronts."

The Ukraine scenario was reminiscent of the Russo-Georgian war of August 2008, during which the government of Tbilisi tried to take back by force its two secessionist territories, South Ossetia and Abkhazia, who have since formally proclaimed their independence and have placed themselves under the military protection of Russia, a fact not recognized by the international community. An annexation of Ukrainian provinces would risk giving way to a new *frozen conflict*[95] in a region that has no shortage of it. In both cases, in Georgia as in Ukraine, the tensions were the result of a standoff between a nationalist camp seeking to emancipate itself from the tutelage of Moscow, and a pro-Russian camp attached to the maintenance of strong political, economic and cultural collaboration with Russia. The first was naturally based on a rapprochement with the United States and the Atlantic Alliance at military level, and with the European Union at economic and commercial level; the prospect of joining the EU signifying in their eyes prosperity, economy, democracy and the end of corruption. The second camp will focus on enhanced cooperation with Russia, which must take measures to guarantee its protection, even its economic integration: distribute Russian passports, promote the use of the Russian language, authorize the posting of Russian troops, join the customs union project which aims to integrate the former Soviet socialist republics (e.g. Belarus, Kazakhstan, Armenia) around Russia.

All the means at Moscow's disposal, political as well as economic, have been used for several years to dissuade its neighbors from approaching the European Union: to blackmail the secessionist territories occupied by Russian troops, Russia imposed a blockade on Georgian and Moldavian wine and on Ukrainian chocolate, then rose the gas prices sold to

[92] Frédéric Charillon, professor of political science and international relations at the University of Auvergne Clermont I, Sciences Politiques Paris and ENA, on the site specialized in international relations *Global Brief.*

[93] *Ibidem.*

[94] In political science, the term *base* refers to a group of voters who almost always support a single party's candidates for elected office. *Base voters* are not likely to vote for the candidate of an opposing party, regardless of the specific views each candidate holds.

[95] In international relations, a *frozen conflict* represents a situation in which an active armed conflict has been brought to an end, but no peace treaty or other political framework resolves the conflict to the satisfaction of the combatants.

Ukraine, threatened Polish apples cultures or discovered the "lack" of hygiene in processing Lithuanian or Belarusian milk, and the list can continue. In November 2013, thanks to continuous economic pressure, they even dissuaded Armenia and Ukraine from signing an association agreement with Brussels: this, in Kiev, was the trigger for the protest movement in the Maidan Square. Only two of the four countries, namely Georgia and Moldova, have finally signed such an agreement with the EU, and the new Ukrainian government is attempting to make the same move.

Another power factor of *Realpolitik* origin: Russia is the successor state of the USSR, and as such has retained a number of its prerogatives. It maintains several military bases abroad, in most of the former republics of the Soviet Union and in Syria. It retains its permanent seat on the UN Security Council and its nuclear arsenal (the largest in the world with more than 16,000 nuclear warheads, 3,500 of which are operational). Russia is one of five countries officially recognized by the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) as having nuclear weapons. Since the fall of the USSR, and despite the decrease in its personnel and budget, the Russian army has remained a leading army on the global scale with more than 1,140,000 soldiers (and two million reservists) and a budget exceeding 70 billion dollars in 2018. On another note, Russia is also, unfortunately, at the head of arms exports with a surplus of 7 to 8 billion dollars, emanating from its armaments sector; its main clients being India, China, Iran, Venezuela and Algeria.

The Russian regime intends to play on all possible levers of power to assert its rank on the international scene. Contrary to what many doctrinarians have suggested, the intervention in Crimea does not constitute a return to the Cold War. Vladimir Putin's nostalgia for Stalin constitutes a well-known fact, as his belief that the fall of the USSR represents *"the greatest catastrophe of the 20th century"*. The regrets of the Russian president do not, however, relate so much to the communist ideology or to the personality of the Father of Nations[96], as to the loss of power of the Russian nation since the 80s and 90s. Vladimir Putin uses the all the weapons which he has at his disposal to preserve Russia's power, authority and interests in its traditional zone of influence, and to discuss on an equal footing with the other great global powers. In a sense, Russia returns more and more to a diplomatic and military strategy already observed in the 19th century, based on solidarity with small allied states (e.g. Serbia, Syria) and on a wider and more flexible network of alliances (with Venezuela, Iran, China), rather than in the logic of two world power blocs that Russia would not have the means to assume.

In the context of the classic paradigms of *power relations* and *power revival*, the Kremlin intends to develop its network of alliances and, to this end, in recent years has even approached controversial players on the international scene.

The Russian proposal to join the customs union and, in 2015, the Eurasian Union, was in fact a last-minute initiative to counter the Eastern Partnership of the European Union. In this respect, Moscow set up a plan to reduce gas prices, to avoid seeing Kiev escape its power, but also to prevent its customs union project from collapsing due to a lack of partners. This aspect was crucial, especially when taking into account that Belarus, Armenia or even Kazakhstan are far from representing the same economic and strategic weight as Ukraine. Russia had therefore accepted a series of almost exorbitant concessions granted to a partner that had been fickle for more than a decade.

Vladimir Putin is now caught in his own trap which prevents him from unblocking the situation in the short term: after having qualified Crimea, in front of tens of thousands of Russians gathered on Red Square in Moscow, like the *"boat which, after a long and painful voyage, has finally returned to its port of origin"*, the master of Kremlin cannot afford to lose face by simply recalling his troops. He would lose popularity not only at home, but also

[96] Due to Lenin's cult of personality he was called Father of Nations.

among Russian-speaking communities in neighboring countries. Putin also knows that the West cannot completely turn his back on him: Russia is not Belarus, Cuba or North Korea. In addition to its place as a supplier of half of Europe in gas and oil, it remains a key player in the resolution of many regional crises, at the head of which is the Syrian conflict and the Iranian nuclear issue. This reality prevents the total ostracization of Russia and limits the options for ending the crisis through dialogue.

4. Conclusions pertaining the how Russian behaviour affects the international legal order and especially the concept of *jus cogens*

Defined in positive law in Article 53 of the Vienna Convention on the Law of Treaties, *jus cogens* norms have been the subject of a multitude of studies and have provoked many doctrinal controversies.

A complete and comprehensive understanding of *"these general imperative rules of law whose failure to comply are likely to affect the essence of the legal order to which they belong, such that the subjects of law cannot but under penalty of absolute nullity, depart from, only by special agreements"*[97], becomes essential in explaining the reasons for their emergence, and their general acceptance, as well as in demonstrating that, despite the consensus surrounding their existence in international law, differences remain as to their content, scope and legal effects. There is a proneness in international law aiming to extend the reach of *jus cogens* indefinitely, well beyond the framework defined by the Vienna Convention and to grant this status to ever more norms of international law.

One can conclude that peremptory norms in international law have an essential role in the organization and cohesion of the international system *in genere*, but also an axiological and almost arcane dimension. *Jus cogens* has been described as a *"set of rules that derive from principles that the legal conscience of humanity considers absolutely essential for coexisting within the international community, at a determined stage in its historical development"*[98]. As a cohesion factor of a developing international community, *jus cogens* have become the standard-bearer of common ideals and collective aspirations. *Jus cogens* constitute the ultimate legal instrument used to exclude and sanction any act which could affect the development of the new international solidarity and security.

The transgression of the law can be at the origin of a transformation process of the norm itself as soon as it meets the adhesion of other state-actors. As certain doctrinarians point out, "*a fact held to be unlawful can become a precedent creating a new norm (...). It is common for a norm to be born illicitly. If opinion juris decides in favor of the new rule, the very notion of legality is amended. Still, the disturbance factor must be monitored. Otherwise, it will remain - whatever his power - a common offender. The fate of the norm will therefore depend on the reactions of other subjects of law and of the international community of jurists, faced with the violation. "*[99] And, this represents exactly the reason due to which the doctrine

[97] Erik, Suy, *Report on Jus Cogens in public international law*, Conference on International Law, Lagonissi, Greece, April 1966, Geneva, European Center for Carnegie Endowment, 1967, p. 3.

[98]Statement by the Representative of Mexico, Mr. Eduardo Suarez to the United Nations Conference on the Law of Treaties, Official Documents, Vienna, March 26-May 24, 1968 and April 9-May 22, 1969, Conference Documents, A/CONF.39/11, p. 319, para. 7.

[99] J. Salmon, *"Introductory reflections on fact and law", in* K. Bannelier, Th. Christakis, O. Corten, P. Klein (eds.), Intervention in Iraq and international law, Paris, Pedone, 2004, p. 3. *See also* E. Giraudpour who affirmed in "Positive law, its relationship to philosophy and politics" that "the fact that a rule of law has suffered serious and repeated violations is not enough to abolish it. All legal rules are intended to be violated. But, as long as the rule of law has retained its value, these violations provoke reactions such as measures of repression against the violators, reprisals, protests which attest to the abnormal and unlawful nature of the violation. On the contrary, when the rule seems to be lost sight of or when a practice contrary to the rule becomes general, the rule in

of obsolescence of the Charter of the United Nations cannot be accepted.[100] It makes a misleading and erroneous assimilation between practice and custom. While, no doubt, a practice of non-compliance with the norms against the use of force exists, the question arises whether there is an *opinio juris* on the issue. Established case law that demonstrates the existence of a customary norm is attested by the cumulative and convergent meeting of each of these two elements: only in the presence of an established practice and an *opinio juris* that a customary norm can be developed. [101]

As the ICJ reiterated, *"the Court does not consider that, for a rule to be established as customary, the corresponding practice must be in absolutely rigorous conformity with the rule. In order to deduce the existence of customary rules, the Court deems it sufficient that the conduct of States should, in general, be consistent with such rules, and that instances of State conduct inconsistent with a given rule should generally have been treated as breaches of that rule, not as indications of the recognition of a new rule. If a State acts in a way prima facie incompatible with a recognized rule, but defends its conduct by appealing to exceptions or justifications contained within the rule itself, then whether or not the State's conduct is in fact justifiable on that basis, the significance of that attitude is to confirm rather than to weaken the rule"*[102].

As we pointed out previously, Russia invoked the principle of self-defence when intervening in the situation in Georgia. The use of self-defence is conditioned both *ratione materiae* and *ratione temporis*. Pursuant to Article 51 of the UN Charter, only an armed assault justifies the use of force in self-defence. However, it was almost thirty years after the entry into force of the Charter that aggression was defined by General Assembly in Resolution 3314[103]. This definition is to say, at least, incomplete because the General Assembly does not draw up an exhaustive list of acts of aggression, contenting itself with giving a non-exhaustive list including invasion, territorial attack, bombardment, maritime blockade or attack by the armed forces of one state against the armed forces of another state. This right of self-defence, whether exercised individually or as part of a military alliance allowing a state, which is not directly affected, to intervene in the name of a defence agreement binding it to the attacked state, which can represent an *alibi* for an intervention not consented, constitutes a natural right according to the Charter, meaning that Article 51 does nothing but to recognize its existence within a conventional framework and its customary value.

Ratione temporis, the drafters of the United Nations Charter conceived self-defence as a kind of time-limited parenthesis, allowing state-actors to react immediately to armed aggression until the Security Council had time to take measures in maintaining the peace, whether coercive or not. Furthermore, and still pursuant to Article 51 of the Charter, the measures taken by member-states in the exercise of this right of self-defence must be immediately brought to the attention of that specific body that can exercise control over these

question has ceased to be part of positive law", *in* Homage of a generation of jurists to President Basdevant, Paris, Pedone, 1960, pp. 210-212.

[100] R. Kolb does not hesitate to call it "false obsolescence". According to him, it is a "very political petition, trying to influence international practice by a kind of pavement thrown into the pond in the hope of inflecting the attitudes of other actors", *in* "Obsolescence in international public law", Paris, Presses de Sciences Politique, 2005, p. 596.

[101] ICJ applies Article 38 (1) (b) of its Statute, according to which custom is "a general practice accepted as law".

[102] ICJ (1986), Judgment on the case concerning *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America), 27 June, http://www.icj cij.org/docket/index.php?case=70, p.108, para. 186.

[103] United Nations General Assembly Resolution 3314 (XXIX) was adopted by the United Nations General Assembly on December 14, 1974 as a non-binding recommendation to the United Nations Security Council on the definition it should use for the crime of aggression.

measures. However, practice shows that the *veto* of one of the five members of the Security Council, Russia being one of them, has the effect of paralyzing any action, rendering it incapable of qualifying a situation or taking the necessary measures to restore peace. These measures are however strongly framed both institutionally and operationally.

Based on Security Council Resolutions 1368 and 1373, which reaffirm the inherent and natural right to self-defence, the United States has developed an extensive concept of self-defence which constitutes an essential part of the *war against terrorism* led by the Bush administration, which resulted in the attack on the Taliban in Afghanistan, considered to be a cradle of terrorism.[104] However, this kind of application of the *precautionary principle*[105] to the use of force is not recognized by international law which requires "armed aggression" as a prerequisite for the right of self-defence. There is, moreover, no precedent that would validate the American thesis since, for example, the bombing, by Israeli aviation of the Iraqi reactor of Osiraq, on June 7, 1981, as preventive self-defence, was violently condemned by the Security Council.[106] An extensive conception of self-defence can also be assimilated to armed reprisals, because of its preventive and repressive characteristics, which are prohibited by international law.[107] Certainly, positive law does not recognize the concept of preventive self-defence thusly it should be obvious that international law appears to be inadequate in the face of the terrorist threat.

Russia's approach regarding *jus cogens* norms is mainly due to the rejection of custom in its view on international law. Russian distrust of rapid developments in international law and new doctrines remains still a constant, as reflected in the statement of the Minister of Foreign Affairs, Sergei Lavrov, at the 67th session of the United Nations General Assembly in 2012: *"No doubt, the legal norms in international affairs will be further adjusted as necessary. But these transformations should be treated with utmost responsibility and full realization of serious risks associated with them. Only consensus can be the criterion for their adoption. Violations of international law should not be portrayed as their 'creative development' ".*

Because of their connections, notably ideological, Russia shares this approach with other powers like China and with third world state-actors. The Russian Federation and China reiterated their adherence to the principles of public international law as expressed in the Charter of the United Nations and the 1970 Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in a Declaration of June 25th 2016[108]. This declaration specifically maintained that "*the principle of sovereign equality is crucial for the stability of international relations"* and condemned unilateral interventions *"as a violation of this principle any interference by States in the internal affairs of other States with the aim of forging change of legitimate governments"*[109].

Although both Russia and China enjoy a permanent seat on the United Nations Security Council, they affirm the shared attachment to sovereignty as a defence against

[104] *See* O., Corten , F., Dubuisson, "Operation "immutable freedom": an abusive extension of the concept of self-defense, Revue générale de droit international public, no. 1, 2002, p. 51-77.

[105] According to the expression of T. Christakis used in "Towards a recognition of the concept of preventive war?", *in* K. Bannelier and T. Christakis, eds., "Intervention in Iraq and international law", Conference of October 17-18, 2003, CEDIN-Paris I, ed. Pedone, 2004, p. 11.

[106] In Resolution 487 of 19 June 1981, the Security Council described this attack as "a clear violation of the Charter of the United Nations and of international standards of conduct".

[107] *See* J.-C Venezia, *"The notion of reprisals in public international law"*, Revue générale de droit international public, 1999, pp. 465-498.

[108] The United Nations General Assembly Resolution 2625, "The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States" was adopted by the General Assembly on 24 October 1970, during a commemorative session to celebrate the twenty-fifth anniversary of the United Nations.

[109] *Ibidem.*

imperialist aims. Indeed, the Chinese approach to international law can be partly explained by its colonial past, notably following the Treaty of Nanking in 1842[110] and the various so-called *"unequal Treaties*"[111].

While the Crimean crisis has seriously undermined the traditional Russian approach to sovereignty as the keystone of international law, it has remained constant in Russian doctrine despite the changes in regimes and the different approaches in international law. As an instrument in rejecting the Western vision in the Soviet approach, the current approach is based on the notion of state sovereignty as the return to the foundations of *jus publicum europaeum*, and thus of Western origin. The primacy of the state sovereignty principle in the Russian approach to international law thus constitutes a synthesis between two opposing ideologies, namely the Soviet one and the other, more conventional, seeking to comply with what considers to be the founding principles of international law, the sovereignty of states being at the heart of the system set up after the Treaties of Westphalia.

Conclusions

The article attempted to demonstrate that if the specific character of *jus cogens*, strictly from a legal point of view, is intrinsically linked to the fact that any particular act or norm deviating from its provisions is null and void, then, specifically, this character which must be clearly established, whenever it is claimed that *"a specific norm of general international law"* also represents a *jus cogens norm*. Such a demonstration is difficult to make with regard to the general principles of law, within the confines of Article 38 of the Statute of the International Court of Justice, which enshrines the principles common to all legal orders, and, therefore, not imposed by the requirements of the international society.

If certain norms are *de jure* absolutely imperative, they most likely would have acquired *customary value*, or would have been enshrined in conventional law. Otherwise, serious doubts can be expressed with regard to their classification in the *jus cogens* category. That's exactly the reason that one should compare them against the norms of conventional law and those of customary law.

The question that arises on the condition that general international law may be of conventional nature, is a question which the International Law Commission did not wish to expressly resolve, although its opinion was reflected in the provisions of the Article 34 of its draft articles, according to which a conventional standard may be extended outside the circle of the contracting parties as a customary rule. In this case at least, a conventional norm can, thanks to this extension, become part of general international law. It will then acquire the character of *jus cogens*, if the treaty which consecrates it expressly provides that any derogation from its provisions will be penalized by *absolute nullity*[112].

In this respect, Article 103 of the Charter of the United Nations has also been frequently invoked. For its part, the International Law Commission did not wish to take a position and, on the contrary, in article 26 paragraph 1 of the draft articles project, left the question open. Article103 does not provide that treaties in conflict with Charter obligations will be null and void, but simply that, in the event of such a contradiction, the provisions of the Charter must prevail. In other words, Article 103 is limited to establishing a simple

[110] The Treaty of Nanjing signed on August 29, 1842, ended the first Opium War and was the first of the so-called *unequal treaties* between China and foreign imperialist powers. China paid the British an indemnity, ceded the territory of Hong Kong, and agreed to establish a "fair and reasonable" tariff.

[111] Unequal treaty is the name given by the Chinese to a series of treaties signed between the Qing dynasty and various Western powers and the Empire of Japan during the 19th and early 20th centuries. All these treaties were concluded after China suffered military defeats or threats by foreign imperialist powers.

[112] Absolute nullity (that could be invoked by any state participating to the treaty, not only by the affected state or *ex oficio*, by an international court and that cannot be covered by confirmation): the constraint exerted on a state representative or exerted on a state for the violation of a *jus cogens* norm.

hierarchy between conventional commitments and those which result from *jus cogens*, because it directly violates the *pacta sunt servanda* standard.

As a matter of fact, Article 103 defines the *constitutional character*[113] of the Charter of the United Nations; if we consider the constitutionality of the Charter through the lens of internal legal order, the conclusion would be that there is a fairly large distance between the concept of constitutional law and that of *jus cogens*.

In respect to customary law, we should emphasize that customary law results from a practice recognized as compulsory, being the expression of a valid legal norm with regard to the society where it was formed, rooted in the consensus from which it benefits within this society. Therefore, what we needed to examine constitutes the content of this consensus.

While there is a conceptual difference between the principles of international law, customary international law and *jus cogens*, it must be understood that these epistemological legal constructions are drenched in the characteristics of the newly formed international milieu post WWII. These concepts were coined, and while the issues pertaining to their future development and evolution were evident to the reputed specialists of the United Nations and of the International Law Commission especially, and exact hierarchy, differentiation or abrupt delimitation between them does not exist. The development of the *jus cogens* normative body would have undoubtable advantages in the promotion of peace and human rights, but there is no clear *formula* as to how norms come acquire such a status. It is why a progressive approach may prove beneficial. Positive law, customary law (or *vice versa*), peremptory norm and finally, *jus cogens*. While this equation may appear simple, to the legal scholar, questions such as maintaining the legitimacy of the international legal order in the context of continuous infringements paralyses such fervent discourses. It is for these reasons that the behaviour of international actors of great magnitude, whether states, international organizations or even liberation movements are crucial to the development of international law.

BIBLIOGRAPHY

1. ****Charter of the United Nations*, 24 October 1945, 1 UNTS XVI.
2. ***Banković and ors v. Belgium and ors, Admissibility, App no 52207/99, ECHR 2001-XII, [2001] ECHR 890, (2007) 44 EHRR SE5, 11 BHRC 435, (2001) 123 ILR 94, IHRL 3273 (ECHR 2001), 12th December 2001, European Court of Human Rights [ECHR]; Grand Chamber [ECHR]
3. ***Law of the Russian Federation on "*The right of citizens of the Russian Federation to move and freely choose their place of residence in the Russian Federation*", 25 June 1993.
4. ****Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, I.C.J. Reports 1996, p. 226, International Court of Justice (ICJ), 8 July 1996, available at: https://www.refworld.org/cases,ICJ,4b2913d62.html [accessed 1 March 2020]
5. ***Case *Georgia v. Russia* (I), Application no. 13255/07, (just satisfaction), ECLI:CE:ECHR:2019:031JUD001325507, Council of Europe Of Human Rights, ECHR, 31 January 2019.
6. ****Burdov v. Russia*, req. 59 498/00, Council of Europe: European Court of Human Rights, 7 May 2002.
7. ****Garabayev v. Russia*, req. 38411/02, Council of Europe: European Court of Human Rights, 7 June 2007.
8. ****Grinberg v. Russia*, req. 23472/03, Council of Europe: European Court of Human Rights, 21 Oct, 2005.

[113] Expression used by M. Virally *in* "Reflections on *jus cogens*", French Yearbook of International Law, Perseé, 1966, p. 5-21.

9. ****Kalashnikov v. Russia*, req. 47 095/99, Council of Europe: European Court of Human Rights, 15Jul, 2002.
10. ****Kuzine v. Russia*, req. 22 118/02, Council of Europe: European Court of Human Rights.
11. 11.****Klyakhin v. Russia*, req. 46 082/99, Council of Europe: European Court of Human Rights.
12. ****Presidential Party of Mordovia v. Russia*, req. 65 659/01, Council of Europe: European Court of Human Rights, Oct 5, 2004.
13. ****Smirnova v. Russia*, req. 46 133/99 and 48 183/99, Council of Europe: European Court of Human Rights, Jul 24, 2003.
14. ****Sukhoruktchenko v. Russia*, req. 69 315/01, Council of Europe: European Court of Human Rights, 10 Feb 2005.
15. ****Troubnikov v. Russia*, req. 49 790/99, Council of Europe: European Court of Human Rights, 5 Jul 2005.
16. ****Znamenskaya v. Russia*, req. 77 785/01, Council of Europe: European Court of Human Rights, June 2, 2005.
17. ***Guide on Article 1 of Protocol No. 1 to the European Convention on Human Rights.
18. ***ICJ (1986), Judgment on the case concerning *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America), 27 June.
19. ***ICJ, Advisory Opinion "*Legality of the threat or use of nuclear weapons"*: Advisory Opinion of 8 July 1996, Rec. ICJ, 1996.
20. ****Isayeva v. Russia,* 57950/00, Council of Europe: European Court of Human Rights, 24 February 2005.
21. ****Issaïeva c. Russie; Youssoupova c. Russie; Bazaïeva c. Russie,* 57947/00; 57948/00; 57949/00, Council of Europe: European Court of Human Rights, 24 February 2005.
22. ***Law of the Russian Federation on "*Recourse to justice against acts and decisions violating the rights and freedoms of citizens*", April 27, 1993.
23. ***Mrs. Wohlwend, Report of the Committee on Legal Affairs and Human Rights, doc. 7,746, Council of Europe Parliamentary Assembly, 2007.
24. ***Opinion of the Committee on Legal Affairs and Human Rights (rapporteur Mr. Bindig), doc. 7, 463.
25. ***Parliamentary Assembly Opinion No. 193 on Russia's application for membership of the Council of Europe, doc. 7, 443.
26. ***Parliamentary Assembly Resolution No. 1,111 on honoring the commitment entered into by Russia when it joined the Council of Europe to establish a moratorium on capital executions, text adopted by the Assembly on 29 January 1997 (5th meeting).
27. ***Preamble of the League of Nations, Covenant of the League of Nations, 28 April 1919.
28. ***Report of the International Law Commission, 1963, General Assembly Doc. of. IT session, supplement No. 9.
29. ***Report of the Political Affairs Committee (rapporteur Mr. Muehlemann).
30. ***Resolutions of the United Nations General Assembly: 2625 (XXV) of October 24, 1970, 2660 (XXV) of December 7, 1970, 3314 (XXIX) of December 14, 1974, A/RES/31/9 of November 8, 1976, A/RES/33/72 of December 14, 1978, A/ RES/42/22 of November 18, 1987.

31. ***Statement by the Representative of Mexico, Mr. Eduardo Suarez to the United Nations Conference on the Law of Treaties, Official Documents, Vienna, March 26-May 24, 1968 and April 9-May 22, 1969, Conference Documents, A/CONF.39/11.
32. ***The 6th Committee of the General Assembly, during the 17th and 21st sessions (cf. P. Raton, Yearbook, 1963 & 1966).
33. ***The Constitution of the Russian Federation, 12 December 1993.
34. ***The Convention (III) on the Opening of Hostilities, The Hague, October 18, 1907.
35. ***The Convention for the Pacific Settlement of International Disputes, The Hague, July 29, 1899.
36. ****The Vienna Convention on the Law of Treaties*, 23 May 1969, United Nations, Treaty Series, vol. 1155, available at: https://www.refworld.org/docid/3ae6b3a10.html [accessed 28 February 2020]
37. *The City of God*, *in Works of Saint Augustine*, 12 vol., Introduction and notes by Bardy, G., translation by Gustave Combès, Paris, Desclée de Brouwer, "Augustinian Library", 1975-1989. 2000.
38. Arend, A. C., *International Law and the Preemptive Use of Force*, The Washington Quarterly, vol.26/2, 2003.
39. Aristotle, "Politics", *introduction and translation* Jean Aubonnet, Paris, Les Belles Letttres, 1971.
40. Benoît-Rohmer, Florence, *Le particularisme du contentieux concernant les pays d'Europe central et orientale*, L'Europe des libertés, no. 9, 2002.
41. Blokker, V. N., *"Is the Authorization Authorized? Powers and Practice of the UN Security Council to Authorize the Use of Force by "Coalitions of the Able and Willing"*, European Journal of International Law, vol. 3/11, 2000.
42. Bolton, J., *Is there really "law" in international affairs*, Transnational Law and Contemporary Problems, vol. 10/1
43. Cassese, A.,*"Article 51"*, *in* J.-P. Cot, A. Pellet, M. Forteau (eds.), The Charter of the United Nations. Article by article commentary, Paris, Economica, 3rd ed., 2005, 2 vol., Vol. I.
44. Christakis, T., *Towards a recognition of the concept of preventive war? in* K. Bannelier and T. Christakis (eds.), "Intervention in Iraq and international law", Conference of October 17-18, 2003, CEDIN-Paris I, ed. Pedone, 2004.
45. Corten, O.,F., Dubuisson, *"Operation "immutable freedom": an abusive extension of the concept of self-defence*", *Revue générale de droit international public,* no. 1, 2002.
46. Daillier, P., Pellet, A., *Droit international public,* Paris, LGDJ, 7th ed., 2002.
47. E. *Suy, The concept of jus cogens in public international law, in* The Gender of *Jus Cogens*, Hilary Charlesworth and Christine Chinkin (ed.), *Human Rights Quarterly* Vol. 15, No. 1 February, 1993.
48. Erik, Suy, *Report on Jus Cogens in public international law*, Conference on International Law, Lagonissi, Greece, April 1966, Geneva, European Center for Carnegie Endowment, 1967.
49. Franck, Th., *Who Killed Art. 2(4)? or: Changing Norms Governing the Use of Force by States*, American Journal of International Law , vol. 64/4, 1970.
50. Giraudpour, E., *Positive law, its relationship to philosophy and politics, in* Homage of a generation of jurists to President Basdevant, Paris, Pedone, 1960.
51. Glennon, M., *How International Rules Die?*, The Georgetown Law J.ournal, vol. 93/3, 2005.
52. Glennon, M., *Limits of Law, Prerogatives of Power. Interventionism after Kosovo*, New York, Palgrave, 2001.

53. Glennon, M., *The Emerging Use of Force Paradigm*, Journal of Conflict & Security Law, vol. 3/11, 2006.
54. Glennon, M., *The Fog of Law: Self-Defence, Inherence, and Incoherence in the United Nations Charter*, Harvard Journal of Law and Public Policy, vol. 25/2, 2002.
55. Glennon, M., *The Rise and Fall of the UN Charter's Use of Force Rules*, Hastings International and Comparative Law Review, vol. 27/3, 2004.
56. Glennon, M., *Why the Security Council Failed*, Foreign Affairs, vol. 82/3, 2003.
57. J.-P. Cot, A. Pellet (eds.), *"Article 2 paragraph 4", in* The Charter of the United Nations. Article by article commentary, Paris, Economica, 2nd ed., 1991.
58. Kant, I., "Project of perpetual peace: A philosophical sketch"(Zum ewigen Frieden. Ein philosophischer Entwurf), text and translation by Jean Gibelin, Paris, Vrin, 1999.
59. Kolb, R., *Obsolescence in international public law,* Paris, Presses de Sciences Politique, 2005.
60. Kovler, A., *The Individual as a Subject of International Law (Discussion Revisited)*, Doctor of Legal Sciences, Professor, Judge of the European Court of Human Rights, Ukraine Law journal, no. 2, 2013.
61. Ksyanov, Rustam, *The Russian Approach to International Law and European Integration*, French Yearbook of International Relations, 2013.
62. Lukashuk, I. I., *The Principle Pacta Sunt Servanda and the Nature of Obligation Under International Law,* The American Journal of International Law, no. 3, 1997. Accessed March 1, 2020. doi:10.2307/2203309.
63. Marochkin, S. J., *International Law in the Russian Courts in Transitional Situations, in* E. Kristjansdottir, A. Nollkaemper and C. Ryngaert (eds.), International Law in Domestic Courts: Rule of Law Reform in Post-Conflict States (Intersentia: Cambridge–Antwerp-Portland, 2012.
64. Miller, M.L.A., Hunter, David, *1875-1961. The Peace Pact of Paris; a Study of the Briand-Kellogg Treaty*, New York; London: G. P. Putnam's & Sons, 1928.
65. N. Schrijver, *"Article 2, paragraph 4" in* J.-P. Cot, A. Pellet, M. Forteau (eds.), The Charter of the United Nations. Article by article commentary, Paris, Economica, 3rd ed., 2005, 2 vol., Vol. I.
66. Pascal, *Pensées*, 1671, posthumous, Brunschwicg (ed.), Paris, Hachette, 1897.
67. Report by Sir Humphrey Waldock, A/CN.4/156, p. 51 and of the two special Rapporteurs, Sir Hersch Lauterpacht and Sir Gerald Fitzmaurice; cf. Dehaussy, Yearbook, 1963.
68. Rostow, E., *The Legality of the International Use of Force by and from States,* Yale Journal of International Law, vol. 10, 1985.
69. Salmon, J., *Introductory reflections on fact and law, in* K. Bannelier, Th. Christakis, O. Corten, P. Klein (eds.), *Intervention in Iraq and international law,* Paris, Pedone, 2004.
70. Schachter, Oscar, *The Lawful Resort to Unilateral Use of Force*, Yale Journal of International Law, Yale, Vol. 10:291, 1985.
71. Tiunov, O. I., *Constitutional Court of the Russian Federation and International Law, PEMII*, 2006.
72. Verhoeven, J., *Public International Law,* Brussels, Larcier, 2000.
73. Virally, M., *Reflections on jus cogens,* French Yearbook of International Law, Perseé, 1966.

CONSIDERATIONS ON GENDER PERSPECTIVE IN INTERNATIONAL HUMANITARIAN LAW

Adrian ALEXE
Lieutenant –colonel Ph.D, senior legal advisor,
International Defence Cooperation Directorate
Ministry of National Defence of Romania
aalexe@mapn.ro

Abstract: *The classical international humanitarian law consecrates women as a category that enjoys special protection, being considered a vulnerable category along with children, the wounded, the sick, the shipwrecked and the prisoners of war. Although they enjoy special protection in international humanitarian law, in recent decades, women continued to be exposed during conflicts and in post-conflict periods to aggressions difficult to imagine. In the last three decades, but especially after the adoption, in the year 2000, of the UN Security Council Resolution 1325, the approach has been revolutionized, meaning that, from the role victim, women should move to the role of leading actors in conflict resolution. The participation of women in decision-making and peace support operations, as well as the integration of the gender perspective in political and military affairs, could be the key to diminishing violence against women during conflict and post-conflict periods. The question that arises is whether the legal basis for such an approach is sufficiently strong to guarantee the universalization of these practices. In our opinion, beyond the discussions on the legal force of UN Security Council resolutions, the main obstacle to universalizing women's participation in decision-making and peace support operations, as well as to gender mainstreaming, lies with deep cultural and axiological differences between democratic societies and other types of societies where women are not given a social role equal to men.*

Keywords: *international humanitarian law, women, peace and security, UNSCR 1325, gender mainstreaming, cultural and axiological differences.*

Introduction

The political history of the last two millennia is a history in which the dominant role of men in political, military and international affairs has created a reality where women have been socially educated to accept a role built on theological, philosophical, political and legal concepts that enshrined the primacy of masculinity.

In traditional societies, women have been assigned an important role within the family, taking care of raising and educating children and maintaining the household.The role of women in society was extremely low, and they did not have political rights until the 20th century.

The development of the notion of gender begins with the movements for the emancipation of women and with the development of anthropological and sociological studies that have as their subject the role of women in society.

Although they have long been considered interchangeable notions, sex and gender are defined differently in the literature, sex being a biological, natural data, and gender a social construct that defines masculinity and femininity based on social roles influenced by cultural, psychological and educational factors.

„The historical events and the European political, social and cultural evolutions created only in the nineteenth century the favorable conditions for the affirmation of women's rights. (...). Starting with this period and in the first decades of the twentieth century, the movements that defended the cause of women were structured and affirmed progressively. Evolving differently, depending on the geographical space, the national specificity, the intellectual origins and the influence of the different political currents (liberal, conservative, socialist), the mode of action and the forms of organization, the feminist discourse manifested

itself at this time as a movement with various claims, especially for the right to vote (granted progressively in most countries in the first half of the twentieth century), improving working conditions and the right to education of women.

After the Second World War and until the 80s of the last century, the women's rights movement had as its main objective the denunciation of (economic, cultural) inequalities and the re-examination of the role of women in society. After 1990, when the initial claims were included in the legal systems and belong to the conventional field of human rights, the feminist movements demand a wide and diverse set of objectives: improving the situation of women, especially vulnerable women, professional equality, sexual freedom, the right to dispose of one's own body. To these parity demands and those related to the development of the notion of gender, the new generation of advocacy movements for women's rights, promoted in the 21st century, adds new themes of reflection and forms of action, which aim in particular at combating violence, sexism and discrimination."[1]

Legal aspects regarding gender issues

The classical international humanitarian law consecrates women as a category that enjoys special protection, being considered a vulnerable category along with children, the wounded, the sick, the shipwrecked and the prisoners of war. Thus, we recall here the provisions of *Article 76, PROTECTION OF WOMEN*, from *Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I)*: „1. Women shall be the object of special respect and shall be protected in particular against rape, forced prostitution and any other form of indecent assault. 2. Pregnant women and mothers having dependent infants who are arrested, detained or interned for reasons related to the armed conflict, shall have their cases considered with the utmost priority. 3. To the maximum extent feasible, the Parties to the conflict shall endeavour to avoid the pronouncement of the death penalty on pregnant women or mothers having dependent infants, for an offence related to the armed conflict. The death penalty for such offences shall not be executed on such women."[2]

Another important moment was the adoption of the Convention for the Elimination of all forms of Discrimination Against Women (CEDAW) adopted and opened for signature, ratification and accession by General Assembly resolution 34/180 of 18 December 1979[3]. The Convention established women's social, economic and political rights, constituting an essential step in the effective promotion of equal opportunities between women and men in all fields of activity. By CEDAW the states have committed to develop appropriate legislation and to apply special measures and actions that will allow to eliminate all forms of discrimination. By establishing international norms and standards, CEDAW also promotes the protection of women during armed conflicts and their participation in peacekeeping and decision-making processes.

Naturally, the next step was to involve women in the decison making process on international peace and security.

Thus, UNSCR 1325/2000 was preceded by the Beijing Declaration and Platform for Action adopted in 1995 at the Fourth World Conference on Women which identified 12 key areas where urgent action was needed to ensure greater gender equality and opportunities.

Among these key areas was mentioned the one regarding *women and armed conflict*

[1] Available on http://www.irdo.ro/femei.php, accessed at 26th of february 2020.

[2] Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of vic tims of international armed conflicts (Protocol I) (with annexes, Final Act of the Diplomatic Conference on the reaffirmation and development of international humanitarian law applicable in armed conflicts dated 10 June 1977 and resolutions adopted at the fourth ses sion). Adopted at Geneva on 8 June 1977.

[3] which Romania signed on September 4, 1980 and ratified on January 7, 1982.

starting from the finding that ”*violations of the human rights of women in situations of armed conflict are violations of the fundamental principles of international human rights and humanitarian law. Massive violations of human rights, especially in the form of genocide, ethnic cleansing as a strategy of war and its consequences, and rape, including systematic rape of women in war situations, creating a mass exodus of refugees and displaced persons, are abhorrent practices that are strongly condemned and must be stopped immediately, while perpetrators of such crimes must be punished.”*[4]

UN Security Council Resolution 1325, adopted unanimously on October 31, 2000, represented a turning point since it was for the first time when this important body for international peace and security addressed the devastating impact of conflict on women.

Following the adoption of UNSCR 1325, the Security Council continued to pay particular attention to issues related to women, peace and security (WPS), adopting a number of other related resolutions, including:

- Resolution 1820/2008 on sexual violence, when used or commissioned as a tactic of war;
- Resolution 1888/2008 mandating the UN Secretary-General to appoint a special representative for combating sexual violence in armed conflicts and establishing a reporting mechanism for the implementation of UNSCR 1820;
- Resolution 1889 of 2009, which reinforces previous resolutions through higher reporting requirements and by encouraging cooperation with Member States and civil society;
- Resolution 1960 of 2010, which has a special role in combating impunity and establishing an annual reporting mechanism for those who have committed sexual assault;
- Resolution 2106 of 2013 which states that sexual violence in conflict should be considered as a war crime and stresses the importance of preventing sexual violence in conflict and bringing the perpetrators to justice;
- Resolution 2122 of 2013, which mainly addresses the importance of full participation of women in the peace process, as well as in other sectors of society;
- Resolution 2224 of 2015 establishing a roadmap for the implementation of UNSCR 1325 and related resolutions to increase women's leadership in the process of peace building and conflict prevention;
- Resolution 2272 of 2016 which encourages the Member States to ensure the eradication of sexual exploitation and violence committed by the personnel of peacekeeping missions and the punishment of the guilty;
- Resolution 2467 of 2019 establishing new measures to eradicate sexual violence and identify support measures for victims.

All these resolutions of the Security Council dedicated to WPS issues are already a coherent system that demonstrates UN's willingness to promote gender mainstreaming in all aspects of international peace and security. Thus, *”the WPS Agenda, consisting of UNSCR 1325 (2000) and its follow-up UNSC Resolutions, broadens the scope of traditional security policy by highlighting the importance of the gender dimension in peace and security. As such, it embodies and catalyses an important paradigm shift in how security and peace should be achieved and sustained. It focuses not only on protecting women and girls from conflict-related violence but also on women's right to participate in decision-making processes. The WPS Agenda stresses that gender equality is embedded in peace and security issues, and that gender perspectives are integral to peace and security. In addition, it states that addressing the gender-related root causes of violence is critical to preventing conflicts.”*[5]

[4] Beijing Declaration and Platform for Action, 1995.

[5] The Council of the European Union conclusions on Women, Peace and Security as adopted at the 3662nd meeting of the Council on 10 December 2018.

The implementation of Resolution 1325 is based on 4 pillars, namely: prevention, protection, participation, restoration and recovery.In implementing the four pillars, as a rule, organizations and states adopt National, Regional and Local Action Plans.

There is a widespread opinion that ”*it is undeniable that UNSCR 1325 represents a milestone in the fight for women's fundamental human rights; however, the level of its significance, considering that it lacks enforcement measures, has repeatedly been called into question by academics and practitioners alike.”*[6]

Although, as we have seen, women enjoy special protection and attention in international human rights and humanitarian law and at the UN level, in recent decades they have continued to be exposed during conflicts and in post-conflict periods to aggressions difficult to imagine, andtheir role in conflict prevention and resolution is still relatively marginal.What causes this condition? Did Resolution 1325 and related resolutions achieve their goal? In the specialized literature there has been since the first years of operation of the UN Security Council a debate on the legal force of these resolutions.

We note here a specialized opinion that reflects the debate around the legal force of the resolutions of the Security Council: ”*The ICJ*[7] *has not definitively decided whether SC decisions possess an overriding binding effect, but it has specified that the binding effect includes, ratione materiae, operational matters and covers, ratione personae, all Member States. Unlike the recommendations of the SC, its decisions have binding force, but the Court has made only a provisional finding that SC decisions have an overriding normative power capable of pre-empting obligations flowing from traditional sources of international law. Recognizing such overriding binding force would give a secondary source of UN law (decisions) a greater normative value than many primary sources of international law (treaties) – thereby giving the SC a potentially very disruptive power – and would ultimately place great faith in the SC truly acting on behalf of all Member States. Ratione materiae, the binding effect of SC resolutions belongs to the realm of international peace and security and includes enforcement under Chapter VII of the UN Charter, but is not limited to that. Since just about any significant international event or situation can be characterized as a threat to peace and security, the scope of the SC's binding powers, if combined with an overriding binding force, would make the SC a dauntingly powerful organ. Whether a specific SC resolution is binding is determined by the language used in it, the discussions leading to it, the Charter provisions invoked, etc., all with the purpose of establishing the intent of the SC. The precise content of the binding effect is left to the SC itself, but the Court has found certain 'implicit' legal effects and, inversely, put some limits on the effects when these conflict with the principles and purposes in Chapter I of the UN Charter. This limitation is too vague to have much practical value in the absence of any organ competent to review the validity of SC resolutions.”*[8]

As far as we are concerned, we agree with a widely shared opinion that only UN resolutions adopted under Chapter VII of the UN Charter (Action with respect to threats to peace, breaches of the peace and acts of aggression) would have binding legal force. As a consequence, Resolution 1325, not being adopted under Chapter VII of the Charter, is not a disposition, but a recommendation.

However, the question that arises is: does the lack of binding legal force make the effects of the Resolution not the expected ones?The answer, in our opinion, is - without any deception - negative.The main argument in favor of this answer is that in the contemporary

[6] On peacewomen.org/resource/un-resolution-1325-significant-lacking, accessed at January 26, 2020.

[7] International Court of Justice.

[8] Marko Divac Öberg, *The Legal Effects of Resolutions of the UN Security Council and General Assembly in the Jurisprudence of the ICJ*, the European Journal of International Law Vol. 16 no.5 © EJIL 2006, pp. 884-885.

world even universal treaties do not produce their full effects in the absence of the states' will to implement them.

In the two decades since the adoption of Resolution 1325, progress has been slow and largely lacking in concrete effects: *„As of December 2019, WILPF (Women's International League for Peace and Freedom-n.n.) analysis shows that 83 UN Member States (43% of all UN Member States) have UNSCR 1325 National Action Plans (NAPs).*

(...) *Of the 83 NAPs adopted to date, only 28 (34%) include an allocated budget for implementation. Furthermore, only 25 NAPs (30%) include references to disarmament and provide specific actions to disarm society. Although civil society has always been at the forefront of efforts to strengthen the implementation of the WPS Agenda, only 62 NAPs (75%) allocate a specific role to civil society in the different stages of the NAP implementation process, with this role often limited to an "advisory" position.*

There are 11 Regional Action Plans (RAPs) in place as well, such as the one of the African Union and of the European Union. Regional coordination efforts also include the Asia-Pacific Regional Symposium on National Action Plans on Women, Peace and Security where the Member States, alongside civil society representatives, share their lessons learned and best practices in the implementation of UNSCR 1325."[9]

Even though UN Security Council Resolution 1325 and related resolutions do not have binding legal force and are not part of International Humanitarian Law, we are still in the presence of **soft law** elements that are coming to strengthen and complement the IHL norms. Also, the IHL norms are complemented by the norms of International Human Rights Law (especially CEDAW).

Conclusions

Although 20 years have passed, the progress is slow and would probably have been equally slow if the WPS Agenda had been based on a legally binding convention. Gender mainstreaming is a long-term process, but it will most likely produce the expected effects because it involves a process of change not only of national law and state policies, but also of mentalities.

Twenty years after the adoption of the Resolution 1325, we can conclude that the legal basis for gender mainstreaming is sufficiently strong to guarantee the universalization of these practices. In our opinion, beyond the discussions on the legal force of UN Security Council resolutions, the main obstacle to universalizing women's participation in decision-making and peace support operations, as well as to gender mainstreaming, lies with deep cultural and axiological differences between democratic societies and other types of societies where women do not enjoy a social role equal to men.

In conclusion, the success of the WPS Agenda should not be sought in over-regulation but in the development, by the relevant international organizations, of those mechanisms that will allow the necessary transformations at the level of those societies where gender discrimination is still practiced.

BIBLIOGRAPHY:

1. *Beijing Declaration and Platform for Action*, 1995.
2. *Convention on the Elimination of All Forms of Discrimination against Women,* adopted and opened for signature, ratification and accession by General Assembly resolution 34/180 of 18 December 1979.
3. Giuliano, Paola, *Gender, An Historical Perspective, UCLA Anderson School of Management, NBER, CEPR and IZA, July 2017.*

[9] On peacewomen.org/member-states, accessed at 09th of February 2020.

4. Kvarving, Lena P. and Grimes, Rachel, *"Why and how gender is vital to military operations"* in PfPC SSRWG and EDWG, Geneva: DCAF and PfPC, 2016.
5. Öberg Marko Divac, *The Legal Effects of Resolutions of the UN Security Council and General Assembly in the Jurisprudence of the ICJ*, the European Journal of International Law Vol. 16 no.5 © EJIL 2006.
6. Onica, Jarka Beatrice Florentina, *Drept internaţional umanitar*, Editura Universităţii „Nicolae Titulescu", Bucureşti, 2013.
7. *Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I),* adopted at Geneva on 8 June 1977.
8. *The Council of the European Union conclusions on Women, Peace and Security* as adopted at the 3662nd meeting of the Council on 10 December 2018;
9. UN Charter, San Francisco, 1945.
10. UN Security Council Resolution 1325/2000.
11. UN Security Council Resolution 1820/2008.
12. UN Security Council Resolution 1888/2008.
13. UN Security Council Resolution 1889/2009.
14. UN Security Council Resolution 1960/2010.
15. UN Security Council Resolution 2106/2013.
16. UN Security Council Resolution 2122/2013.
17. UN Security Council Resolution 2224/2015.
18. UN Security Council Resolution 2272/2016.
19. UN Security Council Resolution 2467/2019.
20. http://www.irdo.ro
21. https://www.peacewomen.org
22. https://www.un.org/en
23. https://www.wilpf.org

NUCLEAR WEAPONS ACTOR IMPORTANT IN *JUS IN BELLO*

Elena SIMION
Mastering the second year, “Carol I” National Defence University
elena.t7@yahoo.com

Abstract: *The topic of nuclear weapons stirs heated debates between the Great Powers, the United States of America and the Russian Federation, as they represent the greatest threat to the security of mankind, although in international law there are no rules expressly prohibiting the use of nuclear and thermonuclear weapons. Their use beyond the necessities of war, causing suffering and irrational damage to humanity and civilization, is contrary to the rules of international law and to the rules of humanity.*

Keywords*: nuclear weapons, humanitarian law, non-proliferation, security environment.*

Introduction

The topic of nuclear weapons stirs heated debates between the Great Powers, the United States of America and the Russian Federation, as they represent the greatest threat to the security of mankind, although in international law there are no rules expressly prohibiting the use of nuclear and thermonuclear weapons. Their use beyond the necessities of war, causing suffering and irrational damage to humanity and civilization, is contrary to the rules of international law and to the rules of humanity.

International law is established by sovereign states. In their cooperation and interaction, there is no international legislative body situated above states. The rules provided for the application of international law are based mainly on the general perception that rules must be respected, establishing a legal framework that each state benefits from in accordance with the principle of multiple reciprocity. Thus, when applying international law norms, there is no apparatus located above states in order to ensure the application of these norms. In some cases, the norms can be applied by constraint, as is the case with the security system established by the UN Charter. Based on the decisions of the Security Council, such measures can be applied, going up to the use of armed force, if peace is threatened or broken or in case of aggression; however, in this case, a mechanism established under a treaty operates within the cooperation between sovereign and equal states, and this organization does not have a superstate nature.

Humanitarian law encompasses all international law norms relating only to the protection during armed conflicts of the persons affected by such conflicts; it also protects the goods that are not directly related to military operations, sometimes using the concept of law of war. “*War is therefore an act of violence, in order to force our adversary to fulfill our will. Violence, i.e., physical violence (because moral violence did not exist outside the concepts of state and law) is therefore the means, and imposing one’s will on the enemy is the purpose*"[1]. Currently, the formula of war is outdated, the war of aggression and the use of force are forbidden, but there may be armed conflicts; the notion of “armed conflict” is broader and corresponds to the broader requirements of potential victims; humanitarian law rules provide protection to victims and minimize negative effects.

[1] Carl von Clausewitz, *„About the war”,* Posthumous opera of General Carl von Clauserwitz, Introductory study, Military Publishing House, Bucharest, 1982, p. 35.

In times of armed conflicts, nuclear weapons are among the non-conventional weapons of mass destruction with particularly destructive and long-lasting effects on the natural environment (together with other chemical agents: dioxin, phytotoxic agents, bacteriological and thermonuclear weapons) and represent a very dangerous war means that affects the environment, due to its uncontrollable nature.

"*A nuclear weapon is an explosive device that releases in an explosive manner the nuclear energy produced by a fission/ fusion chain reaction and is part of the mass destruction weapons category, intended to kill large numbers of people and destroy human-made structures and the biosphere in general*[2]". It also represents any device that can release nuclear energy in an uncontrolled manner and whose set of characteristics make it suitable for war purposes.

Lessons of nuclear disarmament - major part in international security environment strategies

In these times of global change, given the new common threats posed by non-state actors and dangerous regimes, it is necessary to improve the assessment of environmental risks and related regulations necessary for the effective surveillance of existing nuclear sites. "The war" also exists within the relations between some states. However, its operational criteria are different nowadays, due to the change of the type of armed conflicts, with different effects from the previous ones, triggered by the involvement of the UN Security Council, through operations aimed at keeping and restoring or imposing peace and humanitarian action. "*The right to survival*[3]" was launched at the International Court of Justice in The Hague, on the occasion of the advisory opinion requested by the UN General Assembly on the legality or illegality of the use of nuclear weapons. It divided the magistrate's body, as those who support the above concept argue that the state that is on the verge of collapse during an armed conflict has, by virtue of this concept, the right to resort to any means of combat, including nuclear weapons. As a result, the entire norm system of humanitarian law is questioned and represents an attack on the human and material values that they protect, and the presence of the United Nations armed forces in internal conflicts, as the third combatant, brings back into discussion the rules of public international law and implicitly of international humanitarian law. These peacekeeping forces, acting in internal conflicts (Rwanda, Somalia, Bosnia and Herzegovina, Afghanistan, Iraq), had an extremely broad mandate and also exercised humanitarian duties, which through the Conventions of Geneva and their additional Protocols reverted exclusively to the protective powers or to international, impartial and neutral organizations, such as the International Committee of the Red Cross. The main UN body, i.e. the Security Council, holds the monopoly on the exercise of force internationally, being held by the members of the Council. Thus, it tends to concentrate in its hands actions with a humanitarian nature and it has also introduced in international law several considerations of international law, political and military order, contrary to the fundamental principle of humanitarian law, the principle of non-discrimination.

The new threats and challenges to international and national security and to the role of nuclear weapons under current conditions focus on the situation of the nations that hold nuclear weapons. Thus, besides the five states that officially hold nuclear weapons *de jure* (i.e. Russia, the United States, the United Kingdom, France and China), India, Pakistan, Israel and North Korea are considered nuclear *de facto*. India and Pakistan have acknowledged that they carry out military nuclear programs; Israel does not confirm or deny that they have nuclear weapons, and North Korea has claimed that it has obtained such weapons. Besides

[2] Nuclear weapon, nti.org/glossary, accessed at 22.05.2019.

[3] Inna Pascalu, „*The System of International Jurisdiction* ", University of European Studies of Moldova, Faculty of Law, Chişinău, 2013, pp. 4-9.

these states, about 20 countries hold the technological potential to develop nuclear weapons. Whether or not these countries will use their potential depends on the political will of their leaders, the environment of international and regional security, and the degree to which nuclear powers exercise self-restraint. Unlike the Cold War period, nuclear weapons are increasingly presented in official political documents, not as instruments of political isolation, but as combat weapons that can be physically used in order to discourage the escalation of aggression even by conventional means. This situation was considered to be extremely dangerous. The most powerful nuclear arsenals (in Russia and the USA) are still, as in the Cold War, oriented towards each other. This factor, as well as the legacy of the Cold War period regarding partners as potential "nuclear adversaries" strongly hinders the prospects for a true and effective partnership.

The new elements linked to the emergence of extremely precise weapons reduce the possibility to escalate globally these regional conflicts and the crisis of the nuclear non-proliferation regime. Non-proliferation policies are subordinated to the status of political relations, the level of trust among states and their ability to cooperate in order to achieve common goals. Nuclear deterrence is no longer appropriate in a declared partnership between former opponents (first of all Russia and the US); it is not able to deter dishonest states, it is a threat to international security and it is important to counter the most acute threats and modern challenges, especially proliferation and terrorism.

It should be emphasized that, for over 60 years, nuclear weapons have played an important part in preventing regional wars, as well as local conflicts between nuclear powers and their coalitions. Such eloquent examples are the following conflict situations: Taiwan (1954 and 1958), Berlin (1961) and the Cuban missile crisis (1962), whose military-political and ideological confrontations were located between the two world systems. Fortunately, each of these crises ended peacefully and at the same time contributed to the establishment of a system of mutual deterrence and to the conceptual framework of nuclear security. However, at that time, many local wars and armed conflicts began. These included the direct participation of nuclear states: for example, the US and their NATO allies took part in the conflicts in Vietnam and Yugoslavia, and Iraq and the Soviet Union took part in the war in Afghanistan. This shows that the existence of nuclear weapons cannot deter all armed conflicts, let alone terrorist attacks. Therefore, the main purpose of nuclear weapons is to discourage the escalation of conventional wars, i.e. the development of local conflicts in regional areas, and on a large scale, nuclear wars.

Nuclear weapons are a category of weapons, specific war means, different from the other existing means, both in terms of quantity - mass destruction and damage -, as well as in terms of quality - massive thermal effect.

NATO has attached great importance to nuclear disarmament and defence against a nuclear attack, especially since the end of 1954, when the NATO Council authorized the use of nuclear weapons against the signatory states of the Warsaw Pact by NATO commanders, regardless of whether these states used them or not[4]. In 1964, the Secretary of Defence Robert Mc Namara introduced the term Mutual Assured Destruction (MAD) as a basis for the US policy, analyzing new possibilities for increasing the flexibility of American nuclear forces and the challenge of widespread deterrence. The starting point in this strategy was represented by ideas explored by the Multilateral Force - MLF, regarding multilateral nuclear forces, which encompassed all NATO member states and aimed at NATO member countries' access to nuclear weapons control, by placing US nuclear warheads on surface and submarine vessels of NATO multinational crews. However, since NATO member countries had to be

[4] David N. Scwartz, *„NATO'S Nuclear Dilemmas",* Washington, DC: The Brookings Instituition, 1983, p.32.

less able to become independent nuclear capabilities through this strategy, the MLF idea ultimately failed.

In 1967, in order to obtain feedback to the problems arising in the field of nuclear weapons, the Alliance created a forum, in which the United States aimed at presenting to the allies the problems arisen, against the background of the accumulation of nuclear weapons by the USA in Europe; in the early 1970s, the number of nuclear warheads reached over 7300[5]. Later, in 1979, by signing the Strategic Weapons Limitation Treaty - SALT II, the US and the Soviet Union codified the strategic nuclear pact between the two nuclear superpowers. After the Cold War, the NATO leaders approved a new strategic concept of the Alliance, in 1991. It contained three paragraphs and referred to nuclear weapons: "*The Alliance's military forces, which have as their fundamental mission to protect peace, have to provide the essential insurance against potential risks at the minimum level necessary to prevent war of any kind, and, should aggression occur, to restore peace. Hence the need for the capabilities and the appropriate mix of forces already described*"[6].

In April 1999, following NATO's cuts in non-strategic nuclear weapons, NATO leaders revised the 1991 strategic concept, adding that the Alliance simplified the training criteria for its forces with nuclear roles. As a result, the US withdrew several nuclear weapons from Europe (all from Britain and Greece), between 2000 and 2010. In April 2010, at the formal meeting of NATO foreign ministers, they launched a report for a new strategic concept, which provided that the US strategic nuclear forces represent the supreme guarantee of the Alliance's security, but also that "*NATO will preserve a balance between conventional defence forces and nuclear missiles*"[7].

Analyzing the Alliance's nuclear position, the NATO and Washington administrations have taken into consideration possible agreements with Russia in order to pursue a disarmament approach to non-strategic nuclear outbreaks. However, as already mentioned in the 2010 strategic concept, NATO leaders acknowledged that NATO would be a nuclear alliance, as long as there are nuclear weapons in the world.

At the end of March 2016, at the fourth edition of the summit on nuclear security, there was underlined the danger that radioactive substances from over fifty states reach the hands of terrorists. However, the long-term, unanimously accepted objective of the international community is creating a world with fewer nuclear weapons, given that, prior to this summit, the US national strategy for combating terrorism (2011) and the Nuclear Employment Strategy Report (2013) mentioned nuclear terrorism as the greatest threat to the security of mankind.

Legal status

The principle limiting the right to use force was first mentioned in the conventional law at the Hague Peace Conference of 1899[8], and in Article 35 of Protocol 1 to the Geneva Convention, on June 8, 1977[9]; the principle was ratified and developed and it provides that in in any armed conflict, the right of the Parties to the conflict to choose methods or means of warfare is not unlimited. However, it is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary

[5] United States Nuclear Weapons Deployment Abroad, 1950-1977.

[6] NATO, The Alliance's New Strategic Concept, 8 noiembrie 1991, available on http://ww.nato.int//cps/en/natolive/oficial_texts_23847.htm, accessed at 21.02.2020.

[7] NATO, text oficial, Lisbon Summit Declaration Issued by Heads of State and Government in the Meeting of the North Atlantic Council in Lisbon, 20 noiembrie 2010.

[8] Barcroft, Stephen. "The Hague Peace Conference of 1899". *Irish Studies in International Affairs* 1989, Vol. 3 Issue 1, pp. 55–68.

[9] Additional Protocol to the Geneva Conventions of August 12, 1949, on the Protection of Victims, International Armed Conflict (Protocol I) of 08.06.1977, ICRC, International Committee of the Red Cross.

suffering, with non-discriminatory effects (blind, chemical, bacteriological, nuclear and thermonuclear weapons), or to cause widespread, long-term and severe damage to the natural environment.

In international law, there are no rules expressly prohibiting the use of nuclear weapons, but only some partial prohibitions, as follows:

• Experimenting, using, manufacturing, producing or purchasing, receiving, storing, installing, assembling or owning them in certain areas on Earth (Treaties on the Prohibition of Nuclear Weapons in Latin America - Treaty of Tlatelolco, Mexico, 05.12.1967[10] and the Treaty on the prohibition of nuclear weapons in the South Pacific - Rarotonga Treaty, 06.08.1985);

• Placing nuclear weapons and other weapons of mass destruction on the seabed and ocean floor as well as in the subsoil thereof – Treaty on the prohibition of the emplacement of nuclear weapons and other weapons of mass destruction on the seabed and ocean floor and in the subsoil thereof (Seabed Treaty), 11.02.1971 - Moscow, London and Washington[11];

• Placing in orbit around Earth and on any other celestial body any nuclear weapon or any other weapon of mass destruction (Treaty on principles governing the activities of states in the exploration and use of outer space, including the moon and other celestial bodies, 27.01.1967 - Washington, London and Moscow);

• Placing in orbit around the Moon or on any other trajectory in the direction or around the Moon of any object carrying nuclear weapons or using such weapons on the surface or subsoil of the Moon (Agreement governing the activities of states on the Moon and on other bodies celestial, 18.12.1979)[12];

• Nuclear weapons proliferation (Treaty on the non-proliferation of nuclear weapons, 01.07.1968 - Moscow, Washington and London)[13];

• Installing nuclear weapons in Antarctica (Treaty on Antarctica, 01.12.1951-Washington)[14];

• Conducting nuclear experiments (Treaty for the total prohibition of nuclear experiments, adopted at the 51st session of the United Nations General Assembly in September 1996)[15];

- The Geneva Protocol of May 17, 1925, concerning the prohibition of the use of toxic, suffocating or similar gases in war; it was a deterrent factor in the use of these weapons during World War II.

- on November 24, 1961, the UN General Assembly adopted the “Declaration on the prohibition of nuclear or thermonuclear weapons”. It stated that the use of nuclear and thermonuclear weapons is contrary to the spirit of the letter and to other UN purposes; thus, the Charter would be violated if these outweighed war necessities and caused blind destruction and suffering to humanity and civilization, being therefore contrary to the rules of International Law and humanity. The use of nuclear and thermonuclear weapons is directed not only against an enemy or to some enemies, but against humanity in general, given that the peoples of the world not involved in the war will suffer all the ravages caused by the use of these weapons and any state that uses nuclear and thermonuclear weapons shall be seen as violating the UN Charter, acting with contempt against the laws of humanity and admitting a crime against humanity and civilization.

[10] https://www.theguardian.com/cities/from-the-archive-blog/2015/nov/12/guardian-mexico-tlatelolco-massacre-1968-john-rodda, accessed at 22.05.2019.

[11] http://www.europarl.europa.eu/doceo/document/B-8-2019-0131_RO.html, accessed at 22.05.2019.

[12] *Ibidem.*

[13] *Ibidem.*

[14] *Ibidem.*

[15] *Ibidem.*

- Acting in this direction, in 1962, the UN General Assembly adopted a new resolution requesting the Secretary-General to continue to consult the governments of the Member States for views on the possibility of convening a special conference in order to sign a convention on the prohibition of the use of nuclear and thermonuclear weapons for war purposes.

- On January 10, 1969 the UN General Assembly instructed its Secretary-General to prepare, with the help of experts, a report on chemical weapons to be communicated to the Conference of the Disarmament Committee of Geneva, to the Security Council and to the General Assembly.

- On September 26, 1972, the Soviet Union presented a Draft Resolution which, after revision, was adopted on November 29 by Resolution 2936[16], entitled: "*Non*-use of *Force* in *International Relations* and *Permanent Prohibition* of the Use of *Nuclear Weapons*".

Therefore, the position of the 127 non-aligned states must also be recorded: they unanimously consider that the use of nuclear weapons is illegal. In the absence of an express law regarding the use of nuclear weapons, the nuclear club states, especially, but also others, consider that the use of nuclear weapons, especially tactical ones, is legal. All this proves that although there are principles and norms of international law applicable to nuclear weapons and an almost general consensus at the UN and among scientists on the illegal nature of the use of nuclear weapons, the absence of an express rule in this regard has allowed some states to stand and act in the opposite direction.

- The Treaty on the Non-Proliferation of Nuclear Weapons (NPT)[17], which entered into force on 05.03.1970, is the basis of the non-proliferation regime. It recognizes the five permanent member states of the UN Security Council as states that hold weapons: the United States, the Russian Federation, the United Kingdom, France and China (India and Pakistan are not party to this Treaty, and North Korea announced its withdrawal in 2003). The treaty focuses on three main directions: achieving the objective of nuclear disarmament, preventing the proliferation of nuclear weapons and technologies and promoting cooperation in the peaceful use of nuclear energy. Since 1995, the States Parties have extended the treaty indefinitely, organizing meetings called Review Conferences (Rev. Con.) every five years, facilitated by three sessions of Preparatory Committees (Prep. Com.).

Romania ratified the NPT on January 30, 1970 and submitted the instruments of ratification on February 04, 1970, in the capitals of the three storage states (Great Britain, the US and the Soviet Union). Romania supports and attaches equal importance to the three pillars of the NPT (disarmament, non-proliferation, peaceful use of nuclear energy). Our country also held the Presidency of the Second Preparatory Committee (Prep. Com.) of the Review Conference on The Treaty on the Non-Proliferation of Nuclear Weapons, held in Geneva, from 22.04 to 03.05.2013; it also held the position of Vice-President of the third Preparatory Committee, held in New York, from 28.04 to 09.05.2014; at the last NPT Review Conference (2015), Romania held the Presidency of the Main Committee II (Non-Proliferation) through the Permanent Representative of Vienna. At Rev. Con. NPT (2015), Romania presented a National Report attesting the stage of its implementation of the Action Plan adopted at the 2013 Review Conference and co-sponsored the working documents initiated by France, on the Capacity Building Initiative (CBI) under the aegis of the IAEA and the US, with the aim of withdrawing from the Treaty.

In May 2017, at Prep. Com. I, the States Parties met and established the review cycle 2015-2020, whose main objectives remain to ensure NPT validity as the main multilateral instrument of the non-proliferation regime, to maintain the Treaty and to strengthen its implementation.

[16] https://www.un.org/documents/ga/res/27/ares27.htm, accessed at 22.05.2019.

[17] Non-proliferation of nuclear weapons, https://www.mae.ro/node/2010, accessed at 22.05.2019.

- The International Atomic Energy Agency (IAEA) is an independent, intergovernmental, specialized agency of the UN, whose main objective is represented by the cooperation in the nuclear field. It assists Member States in the planning and use of nuclear science and technology for peaceful purposes and facilitates the transfer of nuclear energy technologies to support the development of the thirty-five Member States, chosen on the principle of geographical rotation and meets five times a year (more often only in special situations), the meetings being supervised by the Governing Council.

Romania has been a founding member of the IAEA since 1957, and since 2007 it has implemented the integrated guarantee system (verification), which allows real-time monitoring of nuclear material management. From 01.05.2010, it applies the Agreement on nuclear guarantees and the Additional Protocol thereto, concluded between the EU countries that do not possess nuclear weapons, EURATOM and the IAEA. Romania was part of the Board of Governors from 2008 to 2010 and held the position of President of the General Conference in 2011. It was also part of the control regimes in the field - the Nuclear Suppliers Group (NSG) and the Zangger Committee – and it promotes the international initiatives for the non-proliferation of nuclear weapons (the UN Security Council Resolution 1540, the Global Initiative to Combat Nuclear Terrorism (GICNT) and the Security Initiative on Proliferation - PSI).

- The Treaty on the Total Prohibition of Nuclear Tests (CTBT - Comprehensive Nuclear Test - Ban Treaty), negotiated between 1993 and 1996, was adopted by the UN General Assembly on 10.09.1996. It will enter into force 180 days after its ratification by all the states that have significant nuclear installations. It includes 44 states, including Romania, which signed it on 24.09.1996 and ratified it on 04.10.1999 (Law no. 152/04.10.1999), submitting the ratification instruments on 05.10.1999. The treaty, which has 183 signatory states, has been ratified by 166 countries and stipulates the obligation for the States Parties not to test nuclear weapons on their territory and to refrain from encouraging or participating in nuclear weapons testing.

Romania hosts on its territory a secondary monitoring station - the seismic monitoring station Cheia - Red Mountain. Since 2013, it has been represented in the Group of Eminent Personalities, established with the purpose of supporting the entry into force of the Treaty and was elected to the position of President of the Preparatory Committee of the Treaty Organization on the Total Prohibition of Nuclear Testing (CTBTO), by consensus, at the 45th session of the Preparatory Committee of the CTBTO in Vienna; Romania held this position in 2016.

Nuclear disarmament represents a moral and humanitarian imperative that requires decisive actions, concentrated treaties, capable of building a strong set of global norms that prohibit nuclear weapons for the common good. A legislative approach to the prohibition of nuclear weapons is also the adoption in July 2017 at the UN level of a treaty on the prohibition of nuclear weapons with 122 votes in favor, one vote against and one abstention. The states holding nuclear weapons refused to support this initiative, de facto limiting the scope of the treaty, having in view that North Korea accelerated its weapons program.[18] The treaty will enter into force after 50 states have ratified it[19]. The treaty, which provides for a total ban on the development and threat of the use of nuclear weapons, will apply only to the signatory states. Moreover, the states holding nuclear weapons consider it unrealistic,

[18] Apud Violeta Gheorghe, *The ONU has adopted a treaty to ban nuclear weapons; countries with such weapons have not participated in the negotiations,* Mădălina-Daniela Ghiba, *The Use of Nuclear Weapons in the Light of the International Rules of Law,* in Procedings the 14 th International Scientific Conference „Strategies XXI'' Strategic Changes in Security and International Relations, Volume 2, National Defense University „Carol I'', Security and Defense Faculty, Doctoral School, Bucharest, România, April 2018, p. 239.

[19] *Idem.*

considering that there will be no impact on reducing the current world stock of about 15,000 nuclear warheads[20].

On the other hand, a nuclear war represents an existential threat to the security of human beings, nations and the planet, with a long-term impact on the Earth's ecosystem. It will implicitly target food deficiencies throughout the world and impose changes on the states' policies (even in those countries that hold veto rights in different international Treaties).

Conclusions

The considerable diversification of the risks and threats to global security requires a new trend in the organizational management of armed forces; the controversies around the nuclear issue will continue and it will probably accentuate from a civil perspective, as new nations will develop civil nuclear programs, invoking energy shortcomings, signing civil nuclear agreements. These civil nuclear programs could affect the power balance in this area, due to political and economic reasons (thousands of jobs created), but also taking into account that only adequate economic development can support such programs. Moreover, they may pose threats to the security in areas where these civilian nuclear programs are developed, as they may represent targets for terrorists and may generate subsequent military confrontations, since many of them are initially based on the desire of subjugating populations, conquering territories, acquiring fame. The motivations of the actions aimed at the use of force in order to obtain whatever conquerors want have the most diverse reasons, such the "*splitting hairs*[21]", the respect for human rights and the eradication of terrorism.

BIBLIOGRAPHY

1. Barcroft Stephen,"*The Hague Peace Conference of 1899*", Irish Studies in International Affairs 1989, Vol. 3 Issue 1.
2. Carl von Clausewitz,„*About the war", Posthumous opera of General Carl von Clauserwitz, Introductory study, Military Publishing House, Bucharest*, 1982.
3. David N. Scwartz, „*NATO'S Nuclear Dilemmas*", Washington, DC: The Brookings Instituition, 1983.
4. Violeta Gheorghe, *ONU a adoptat un tratat de interzicere a armelor nucleare; ţările care deţin astfel de arme nu au participat la negocieri [The UN has adopted a treaty for the prohibition of nuclear weapons; the nuclear weapon countries did not participate in the negotiations],* article.
5. Mădălina-Daniela Ghiba , Toma PLEŞANU, *The Use of Nuclear Weapons in the Light of the International Rules of Law* [Procedings the 14 th International Scientific Conference „Strategies XXI'' Strategic Changes in Security and International Relations, Volume 2, National Defence University „Carol I'', Security and Defence Faculty, Doctoral School, Bucharest, România], 2018.
6. Herodot, "*Histories*", volume I - "Clio", Teora Publishing House, Bucharest, 1998.
7. Inna Pascalu „*The System of International Jurisdiction*", University of European Studies of Moldova, Faculty of Law, Chişinău, 2013.
8. Additional Protocol to the Geneva Conventions of August 12, 1949, on the Protection of Victims, International Armed Conflict (Protocol I) of 08.06.1977, ICRC, International Committee of the Red Cross (Additional Protocol to the Geneva Conventions of August 12, 1949, on the Protection of Victims,

[20] *Idem.*

[21] Herodot, "*Histories*", volume I - "Clio", Teora Publishing House, Bucharest, 1998, p. 145.

International Armed Conflict (Protocol I) of 08.06.1977, ICRC, International Committee of the Red Cross).

9. NATO, text oficial, Lisbon Summit Declaration Issued by Heads of State and Government in the Meeting of the North Atlantic Council in Lisbon, 20 noiembrie 2010 (NATO, official text, Lisbon Summit Declaration Issued by Heads of State and Government at the North Atlantic Council Meeting in Lisbon, November 20, 2010).
10. United States Nuclear Weapons Deployment Abroad, 1950-1977.
    1. 11.http://ww.nato.int//cps/en/natolive/oficial_texts_23847.htm, NATO,TheAlliance's New Strategic Concept, 8 noiembrie 1991.
11. Nuclear weapon, nti.org/glossary.
12. https://www.theguardian.com/cities/from-the-archive-blog/2015/nov/12/guardian-mexico-tlatelolco-massacre-1968-john-rodda.
13. http://www.europarl.europa.eu/doceo/document/B-8-2019-0131_RO.html.
14. https://www.un.org/documents/ga/res/27/ares27.htm.
15. https://www.mae.ro/node/2010.

BOSNIA AND HERZEGOVINA – SEXUAL VIOLENCE AS WEAPON OF WAR

Daniela Vetina ENE
Masterand, SMMC 21, National Defence University „Carol I”,
daniela.ene65@gmail.com

***Abstract**: The use of rape during the war in Bosnia is not a by-product of conflict, but a pre-planned and deliberate military strategy, part of a systematic policy of ethnic purification with the conscious intention to demoralize and terrorize communities, and to demonstrate power invading forces. The first purpose of these mass rapes is to instill terror in the civilian population, with the intention of forcibly displacing them on their property. The second goal is to reduce the likelihood of return and reconstitution by applying humility and shame on the target population. These effects are strategically important for non-state actors, as they need to eliminate the targeted population from that territory. The use of mass rape is well suited to campaigns involving ethnic cleansing and genocide, as the goal is to destroy or forcefully remove the target population and ensure that they will not return.*

***Keywords**: rape wartime, pre-planned strategy, ethnic cleansing, humility, stigma, genocide.*

Introduction - A short history

In war the battles are fought with rifles, grenades and threats. War means large number of victims, attacks, dissimulation and many refugees. But there is another battlefield as well: the women's and children's bodies. The subject is so delicate that it rarely reaches the history books, the full attention of the court or in the press. Since there are wars in the world, sexual violence is part of it.

Armed conflicts have rules in accordance with international law. The law is clear: *“rape or any other form of sexual assault is prohibited*" said in a February 2019 speech, Peter Maurer - president of the International Committee of the Red Cross. "*The prohibition, clear and general in character, can be found in the Geneva Conventions. However, even today we are facing failures and lack of responsibility*".[1] Often, the reality of modern warfare is fronts that separate and conflicts that extend over the civilian population.

“*There are women living among us who are victims of wartime rape. But if you’re not recognized and feel like a victim again, it is easier for you to stay quiet. So everyone stays silent about it. And that is the most distressing side of it, when everyone is silent.”*[2] Stinojka Tešić, Bratunac Women's Forum, interviewed by Amnesty International in April 2012.

As in other countries of the ex-Yugoslavia, Bosnia and Herzegovina is still facing to the legacy of the crimes committed during the 1992-1995 war. One of the least overlooked, but most keenly felt, injustices is the ongoing failure to provide survivors of war rape and other forms of sexual violence, the moral and material reparation they desperately need - and to which they are entitled under of international law.

Following the 1992-1995 war in Bosnia and Herzegovina, Amnesty International gathered a significant amount of evidence confirming that crimes of sexual violence have been committed. The organization continued to collect numerous testimonies of women who

[1] Maurer, Peter, President of the International Committee of the Red Cross, “*Standing together against sexual and gender-based violence*, Speech, 25th February, 2019, https://www.icrc.org/en/document/speech-icrc-president-joint-event-sexual-and-gender-based-violence-un-secretary-general , accessed at 27th February 2020.

[2] “*When everyone is silent – reparation for survivors of wartime rape in Republic Srpska in Bosnia and Herzegovina*”, Amnesty International Publications, 31st October 2012, https://www.amnesty.org/en/documents/EUR63/012/2012/en/, accessed at 27th February 2020.

were subjected to torture, including rape, which was often systematic and repeated, sexual slavery, forced pregnancy and other crimes of sexual violence. Since the end of the war, Amnesty International has been asking the authorities in Bosnia and Herzegovina to investigate those who might be responsible for these crimes in effective and impartial criminal cases and to provide survivors access to effective redress.

Violence assumed a gender-oriented form through the use of rape during the Bosnian war. While men from all ethnic groups committed rape, the vast majority of rapes were committed by Bosnian Serb forces in the Srpska Republic Army (SPV) and Serbian paramilitary units, which used genocidal rape as an instrument of terror, as part of their ethnic cleansing program.[3] Estimates of the number of women raped during the war range from 12,000 to 50,000.[4]

The International Criminal Tribunal for the Former Yugoslavia (TPIY) declared that "*systematic rape*" and "*sexual enslavement*" during the Bosnian wartime were considered - first, "crimes against humanity" and secondly, "*genocide crimes*".[5] Although TPIY did not treat mass rapes as genocide, many concluded that due to the organized and systematic nature of mass rapes of the Bosnian population (Bosnian Muslims), these rapes were part of a larger genocide campaign and that the VRS were conducting a policy of genocidal rape against Bosnian Muslim ethnic group.

The trial of the commander of a tactical unit of the Bosnian Serb Army (VRS) Dragoljub Kunarac was the first time, in any national or international jurisprudence, according to which a person was convicted for using rape as a weapon of war. The widespread mass-media outrage of Serbian atrocities by paramilitary and military forces against Bosnian women and children has attracted international conviction of Serbian forces.[6]

According to Amnesty International, the use of rape during the wartime is not collateral to the conflict, but a pre-planned and deliberate military strategy. The first purpose of these mass rapes is to instill terror in the civilian population, with the intent of forcibly displace them from their property. The second goal is to reduce the probability of return and reconstitution by inflicting humility and shame on the targeted population. These effects are strategically important for non-state actors, as they need to eliminate the targeted population from the territory. The use of mass rape is well suited for campaigns involving ethnic cleansing and genocide, as the aim is to destroy or forcefully eliminate the targeted population and ensure that they will not return.[7]

Historian Niall Ferguson assessed a key factor behind the high-level decision to use mass rape for ethnic cleansing as a wrong nationalism[8]. From the very beginning of its history, Yugoslavia has not been a platform for domestic nationalist feelings, and people who sought to ignite tensions were at risk of imprisonment, torture or execution. In 1989, Serbian President Slobodan Milošević ignited the Serbian nationalist feeling with the "*Gazimestan Speech*"[9] at 600th anniversary of the Battle of Kosovo. The feelings of victimhood and aggression towards Bosnians were further mixed with exaggerated stories about the role

[3] Totten, Samuel, Bartrop, Paul R., "*Dictionary of Genocide*", 2007, pp. 356-357; Henry, Nicola, "*War and Rape: Law, Memory, and Justice*", Routledge, 2010, p. 65.

[4] Crowe, David M., "*Crimes, Genocide, and Justice: A Global History*" Palgrave Macmillan, 2013, p. 343.

[5] Cohen, Philip J., "*The Complicity of Serbian Intellectuals*", In Cushman, Thomas, Mestrovic, Stjepan G. (Eds.), "*This Time We Knew: Western Responses to Genocide in Bosnia*" New York University Press, p.47.

[6] Stiglmayer, Alexandra, "*The Rapes in Bosnia-Herzegovina*". In Stiglmayer, Alexandra (Ed.). Mass Rape: The War against Women in Bosnia-Herzegovina. University of Nebraska Press., 1994, p. 202.

[7] Parliamentary Assembly of the Council of Europe. Resolution 1670 (2009). Sexual violence against women in armed conflict. Adopted on 29 May 2009, para. 6.

[8] Ferguson, Niall, "*The War of the World: History's Age of Hatred*", Penguin Morales, 2009, p. 180.

[9] Ferguson, Niall, "*The War of the World: Twentieth-Century Conflict and the Descent of the West*", Reprint ed., Penguin, 1996, p. 627.

played by a small number of Bosnians in the persecution of Serbs during the Ustaše genocide of the 1940s.[10] Serbian propaganda suggested that Bosnians were descended, largely, from the Turks. Despite hate campaigns led by the Serbian government, some Serbs tried to defend Bosnians from atrocities and had to be threatened, including when troops announced by loudspeakers that "*every Serb who protects a Muslim will be killed immediately*".[11]

Examples regarding the violation of the norms of international humanitarian law

Before the conflict began, citizens of Bosnian ethnicity have already started to be fired, ostracized and to reduce their freedom of movement. At the beginning of the war, Serbian forces began to target the Bosnian civilian population. Once cities and villages were besieged, the military, the police, the paramilitaries and sometimes even Serb villagers continued these attacks. Bosnian houses and apartments were totally looted or destroyed, the civilian population was surrounded and some were physically abused or killed during the conflict.[12] Men and women were separated and then held in concentration camps.

Estimates of the number of women and girls raped range from 12.000 to 50.000, the large majority being Bosnians raped by Bosnian Serbs. UNHCR experts have claimed 12.000 rapes. The European Union estimates a total of 20.000, while Bosnia's Interior Ministry claims 50.000. The UN Experts Commission has identified only 1.600 cases of sexual violence.[13]

Serbian forces set up "*rape camps*", where women were subjected to repeated rape and released only when they were pregnant. The abduction of Bosnians of Muslim origin and public rape in front of villagers and neighbors were not uncommon. On October 6th, 1992, the UN Security Council established a Commission of Experts headed by Sheriff Bassiouni. According to the Commission's conclusions, it was obvious that the rape was systematically used by the Serbian forces and had the support of local commanders and authorities. The Commission also reported that some criminals said they were ordered to rape and the use of rape was a tactic to ensure that the Bosnian Muslim population would not return to the former residence area. The attackers told the raped victims that they would be released only if they bear a child with the attacker's ethnicity. Pregnant women were detained until it was too late to interrupt their pregnancy. The victims were told that they would be hunted down and killed if they reported what happened.

"In Bosnia, some of the reported rape and sexual assault cases committed by Serbs, mostly against Muslims, are clearly the result of individual or small group conduct without evidence of command direction or an overall policy. However, many more seem to be a part of an overall pattern whose characteristics include: similarities among practices in non-contiguous geographic areas; simultaneous commission of other international humanitarian law violations; simultaneous military activity; simultaneous activity to displace civilian populations; common elements in the commission of rape, maximizing shame and humiliation to not only the victim, by also the victim's community; and the timing of the rapes. One factor in particular that leads to this conclusion is the large number of rapes which occurred in places of detention. These rapes in detention do not appear to be random, and they indicate at least a policy of encouraging rape supported by the deliberate failure of camp commanders

[10] *Ibid*, p. 206.

[11] Ferguson, Niall, *"The War of the World: History's Age of Hatred",* Penguin Morales, 2009, pp. 626-631.

[12] Steven L. Burg; Paul S. Shoup, *"Ethnic Conflict and International Intervention: Crisis in Bosnia-Herzegovina, 1990-93",* Taylor & Francis, 2015, p. 222.

[13] Crowe, David M., *"War Crimes, Genocide, and Justice: A Global History",* Palgrave Macmillan, 2013, p. 343.

and local authorities to exercise command and control over the personnel under their authority."[14]

The commission's conclusions were: "*Rape has been reported to have been committed by all sides to the conflict. However, the largest numbers of reported victims have been Bosnians, and the largest numbers of alleged perpetrators have been Bosnian Serbs. There are few reports of rape and sexual assault between members of the same ethnic group*."[15]

In 1993, the investigators of the European Community, Simone Veil and Anne Warburton, concluded in the report that rape by Bosnian Serb forces was not a side effect of the conflict, but was part of a systematic ethnic cleansing policy and was "*with the conscious intention of demoralizing and terrorizing communities, relocating them from their home regions and demonstrating the power of invading forces*".[16] Amnesty International and Helsinki Watch also concluded during the conflict that rape was being used as a "*war weapon, the main purpose being to cause humiliation, degradation and intimidation to ensure that survivors would leave and never return*".[17] Throughout the conflict, women from all ethnic groups were affected, but not at the level at which the Bosnian population suffered.

The testimony of a survivor of the Klainovik camp - where about 100 women have been detained and subjected to "*group rape*" - pointed out that the rapists continually told to their victims: "*You are going to have our children of our ethnicity*" and the reason they being raped was "*to plant the seed of the Serbs in Bosnia*".[18] Women were forced to leave camp after long term, with advanced pregnancies and give birth to children as a result of these group rapes. Many of the reports of the abuse have illustrated the ethnic dimension of wartime rapes.

"*The women knew the rapes would begin when "Marš na Drinu" was played in the main mosque's loudspeaker. Marš Na Drinu / The march to Drina is a former Chetnik fighting song (Slavic nationalist guerrilla force in the Balkans, active during World War II, banned during the Tito's time. While Marsh was played, the women were ordered to undress and the soldiers entered the houses, taking the ones they wanted. The age of abducted women ranged from 12 to 60 years. Frequently, the soldiers would seek out mothers-daughters combinations, which were severely beaten during the rapes."*[19]

Serb forces set up camps where rapes took place, such as those in Keraterm, Vilina Vlas, Manjača, Omarska, Trnopolje, Uzamnica and Vojno. "*At Keraterm camp, some guards raped a detained woman, on a table, in a darkened room, until she lost consciousness. The next morning, she found herself lying in blood.*"[20] In May 1992, Serb villagers from Snagovo, Zvornik, surrounded and captured the village of Liplje and turned it into a concentration camp. More than four hundred people were imprisoned in several houses, and those held there were subjected to rape, torture and crime.

[14] Allen, Beverly, "*Rape Warfare: Hidden Genocide in Bosnia-Herzegovina and Croatia*", University of Minnesota Press, 1996, p. 47.

[15] *Ibid,* pp. 77-78.

[16] Full Warburton Mission II Report, February 1993, EC Investigative Mission into the treatment of Muslim Women in the Former Yugoslavia: Report to EC Ministers, http://www.womenaid.org/press/ info/ human rights/warburtonfull.htm, accessed at 27th February 2020.

[17] "*When everyone is silent – reparation for survivors of wartime rape in Republic Srpska in Bosnia and Herzegovina*", Amnesty International Publications, 31st October 2012, https://www.amnesty.org/en/documents/ EUR63/012/2012/en/, accessed at 27th February 2020.

[18] P.A.Weitzman, "*The politics of identity and sexual violence: A review of Bosnia and Rwanda*", 2008, Human Rights Quarterly, 30, pp. 561-578.

[19] "*Seventh Report on War Crimes in the Former Yugoslavia: Part II*". US submission of information to the United Nations Security Council, 1993, https://phdn.org/archives/www.ess.uwe.ac.uk/documents/sdrpt7a.htm, accessed at 22nd May 2019.

[20] Edina Becirevic, "*Genocide on the Drina River*", New Haven, CT: Yale University Press, 2014, p. 173.

In early 1992, between 5.000 and 7.000 Bosnians and Croats were detained in camps in inhumane conditions at Omarska. In this camp, the rape, the sexual assaults and torture of men and women were not uncommon. One newspaper described the events there as "*the location of an orgy of killing, mutilation, beating and rape*". At the Trnopolje camp, an unknown number of women and girls were raped by Bosnian Serb soldiers, police officers and camp guards. In the Uzamnica camp, a witness in the trial of Oliver Krsmanovič, accused of crimes related to the massacres in Visegrad, claimed that male detainees were at one time forced to rape women.[21]

Detention camps were set up in the town of Foča, controlled by the Serbs. While kept at one of the town's most known rape camps in "*Karaman House*", Bosnian women, including children under the age of 12, were repeatedly raped. During the trial of Dragoljub Kunarac and others, the conditions of these camps were described as "*intolerably unhygienic*" and the Foča police chief, Dragan Gagović, was identified as one of the person who would visit these camps, where he would select women, take them outside and then rape them. "*Women were kept in various detention centers where they had to live in intolerably unhygienic conditions, where they were mistreated in many ways including, for many of them, being raped repeatedly. Serb soldiers or policemen would come to these detention centers, select one or more women, take them out and rape them ... All this was done in full view, in complete knowledge and sometimes with the direct involvement of the local authorities, particularly the police forces. The head of Foča police forces, Dragan Gagović, was personally identified as one of the men who came to these detention centers to take women out and rape them.*"[22]

The Croatian forces set up concentration camps at Chelebići, Dretelj, Gabela, Rodoč, Kaonik, Vitez and Žepa. In Čelebići camp, Serbian civilians were subjected to various forms of torture and sexual abuse, including rape. In Dretelj, most of the detainees were Serb civilians, held in inhumane conditions, and the detainees were raped and told they would be held until an "*Ustaša*" was born. Both Serbian and Bosnian civilians were detained in the Rodoč camp and reported being sexually assaulted. In Doboj, Bosnian Serb forces separated women from men and then facilitated rape of some women by members of their male family.[23]

An unknown form of rape in the wartime was that committed against men and boys. Although no concrete number has been established, it is estimated that about 3.000 were raped during the conflict. Moreover, it is assumed that hundreds, even thousands of victims have never come forward because of their deaths, as well as the stigma regarding sexual abuse. Many male victims have been ostracized in their communities, often being publicly naked or accused of homosexuality, due to the predominantly male culture in Bosnia. The range of abuses has varied greatly. Some victims were sexually tortured, while others were forced to torture other prisoners. The facts included forcing oral and anal sex, genital mutilation and severe trauma to the genitals. The motives of these crimes mainly concerned humiliation and asserting domination over victims, rather than the perpetrators' sexual satisfaction. The trauma resulting from these crimes included a number of mental and physical health issues, including feelings of hopelessness, flashbacks, sexual dysfunction.[24]

Following the end of hostilities, with the signing of the Dayton Agreement in 1995, have been sustained efforts to reconcile ethnic factions. Particular attention was paid to the

[21] Henry, Nicola, "*War and Rape: Law, Memory, and Justice*" Routledge, 2010, pp. 66-67.

[22] Tausan, Marija, "*Defense Witnesses Speak about Abusers in Uzamnica*", BRIN, 20th August 2013.

[23] Abu-Hamad, Aziz, "*Rape as a Weapon of War*". The Human Rights Watch Global Report on Women's Human Rights (PDF), Human Rights Watch, 1995.

[24] "*Legacies and Lessons: Sexual violence against men and boys in Sri Lanka and Bosnia & Herzegovina*" (PDF), UCLA School of Law: Health & Human Rights Project. All Survivors Project, https://williamsinstitute.law.ucla.edu/wp-content/uploads/Legacies-and-Lessons-May-2017.pdf, accessed at 12th May 2019.

need to understand what happened during the conflict, to have the responsible leaders brought to justice and to accept their guilt for mass rapes and the other atrocities.

As a result of the conflict, ethnic identity is now of much greater social importance in Bosnia than before 1992. From the 1960s to the beginning of the war, nearly twelve percent of marriages were mixed between members of different communities and young citizens would be they often refer to themselves as Bosnians, rather than identifying their ethnicity. After the conflict, it was effectively mandatory to be identified as a Bosnian, Serbian or Croatian and this was a problem for the children of rape victims, as they reached the full age.[25]

A medical study of 68 victims of rape - Croatians and Bosnians - during the Bosnian wartime, found that many of them suffered psychological problems. No one had a psychiatric history before rape. The study concluded that rapes had "*immediate and long-term profound consequences on women's mental health*".[26]

In the post-war years, Bosnian society strives to overcome this collective tragedy of war. The rape, in the Bosnian war, was intended not only to take the victims' bodies, but also their souls, their identity and their existence. It was used as a "war weapon", which affected the common consciousness of the Bosnian people. As Pierre Bayard states, "*In Bosnia, rapes not only accompanied the advance of Serbian armies, but also the result of a concerted policy of cultural eradication.*"[27] In other words, rape itself served as a tool for strategic desecration of Bosnian identity and any connection with it.

In the study entitled "*Mass rape: the war against women in Bosnia and Herzegovina*", Alexandra Stiglmayer concludes: "*In Bosnia-Herzegovina and Croatia, rape has been an instrument of 'ethnic cleansing*." The UN Commission of experts that investigated the rapes in former Yugoslavia has concluded: "*Rape cannot be seen as incidental to the main purpose of the aggression but as serving a strategic purpose in itself"*.[28] The report of the humanitarian organization Amnesty International states: "*Instances that have included sexual infringements against women are apparently part of an inclusive pattern of war conduct characterized by massive intimidation and infringements against Bosnians and Croats*."[29] The American Human Rights Organization - Helsinki Watch believes that rape is being used as a "*weapon of war*" in Bosnia-Herzegovina: "*Whether a woman is raped by soldiers in her home or is held in a house with other women and raped over and over again, she is raped with a political purpose – to intimidate, humiliate, and degrade her and others affected by her suffering. The effect of rape is often to ensure that women and their families will flee and never return*." Against this background, it is obvious that rapes in Bosnia-Herzegovina are taking place "*on a large scale*" (UN and UE), that they

[25] Saunders, Doug (5 April 2009), "*Children born of rape come of age in Bosnia*", Globe and Mail, https://www.theglobeandmail.com/incoming/children-born-of-rape-come-of-age-in-bosnia/article1096015/, accessed at 20th May 2019.

[26] Lončar, Mladen, Medved, Vesna "*Psychological consequences of rape on women in 1991–1995 war in Croatia and Bosnia and Herzegovina*" Croatian medical journal 47 (2006), pp. 67–75, https://www.ncbi.nlm.nih.gov./pmc/articles/PMC2080379/, accessed at 12th May 2019.

[27] Bayard, Pierre, "*Collective Rape and Post memory in Bosnia*", Journal of Literature and Trauma Studies 4(2015), pp.115–123, https://muse.jhu.edu/article/621142, accessed at 20th May 2019.

[28] Letter dated 24 May 1994 from the Secretary-General to the President of the Security Council, S/1994/ 674, 27 May 1994, https://www.icty.org/x/file/About/OTP/un_commission_of_experts_report1994_en.pdf, accessed at 27th February 2020.

[29] "*Bosnia-Herzegovina - Gross abuses of basic human rights*" Report AI Index: EUR 63/01/92, Amnesty International October 1992, https://www.amnesty.org/download/Documents/192000/eur630011992en.pdf, accessed at 22nd May 2019.

are acquiring a systematic character, and that "*in by far the most instances Muslim Bosnian women are the victims of the Serbian forces*" (Amnesty International).[30]

In August 1992, mass-media stories publicized the use of rape as a war strategy and one of the first to bring it to the attention of the world was the Newsday Program correspondent - Roy Gutman, in 1992 "*Mass Rape: Muslims Recall Serb Attacks*".

The UN Security Council established the TPIY in response to the conflict's human rights violations in the former Yugoslavia. Article 5 of the TPIY Charter clarified that the Court had the power to prosecute war crimes, and the Charter specifically condemned rape as a crime, for which people can be charged.

A CIA report "leaked" in 1995, concluding that Serbian forces were responsible for 90% of the atrocities committed during the conflict in Bosnia.

Following the siege of Srebreniča in July 1995, Madeleine Albright, the United States ambassador to the United Nations- at the time, told the UN Security Council that "*the location of about 6.000 Bosnians - men and boys - in Srebreniča was unknown, but their fate was not. They have enough information to conclude now that Bosnian Serbs have beaten, raped and executed many of the refugees."*[31] In the early 1990s, calls were made for legal action to be taken over the possibility of genocide having occurred in Bosnia. The TPIY set the precedent that rape in warfare is a form of torture.

By 2011, TPIY had indicted 161 people from all ethnic factions for war crimes and heard the statements of more than 4.000 witnesses. In 1993, TPIY defined rape as a "*crime against humanity*" and also defined rape, sexual slavery and sexual violence as "*international crimes*" that constitute "*torture and genocide*". TPIY judges ruled during Dragoljub Kunarač, Radomir Kovač and Milorad Krnojelač trial that rape was used by Bosnian Serb armed forces as "*an instrument of terror*": Kunarač was sentenced to 28 years in prison for rape, torture and slavery. Kovač, who raped a 12-year-old boy and then sold him into slavery, was sentenced to 20 years in prison and Krnojelač to 15 years. TPIY said "*harsh persecution orgy*" was held in various camps in Bosnia.[32]

Criminal investigation and prosecution of the perpetrators under international law is an essential component of the remedies that the survivors of these offenses are entitled to. It is an obligation that the authorities of Bosnia and Herzegovina and its constituent entities fail to fulfill to the end. Of the tens of thousands of alleged crimes of sexual violence against women and girls during the war, less than 40 cases have been prosecuted by the International Criminal Tribunal for the Former Yugoslavia (TPIY) in The Hague or by state courts and entities in Bosnia and Herzegovina, starting with 1995.[33]

[30] Stiglmayer, Alexandra, "*The Rapes in Bosnia-Herzegovina*", In Stiglmayer, Alexandra (Ed.), "*Mass Rape: The War against Women in Bosnia-Herzegovina*", University of Nebraska Press, 1994, pp. 82–169.

[31] Security Council strongly condemns humanitarian law violations by Bosnian Serbs, Paramilitary Forces; Cities summary executions, mass expulsions, Press release SC 6149, 21st December 1995, https://www.un.org/ press /en/1995/19951221.sc6149.html, accessed at 20th May 2019.

[32] Buss, Doris, "*Prosecuting Mass Rape: Prosecutor v. Dragoljub Kunarac, Radomir Kovac and Zoran Vukovic*", Feminist Legal Studies. 10 (1), 2002, pp. 91–99, https://link.springer.com/article/10.1023%2FA %3A10 14965414217, accessed at 20th May 2019.

[33] Escritt, Thomas, Zuvela, Maja "*Bosnian Croat leaders jailed for 1990s ethnic cleansing*". Reuters,29th May 2013, https://www.reuters.com/article/us-warcrimes-bosnia-prlic/bosnian-croat-leaders-jailed-for-1990s-ethnic-cleansing-idUSBRE94S0L920130529, accessed at 20th May 2019; International Criminal Tribunal for the former Yugoslavia, "*About the ICTY*," available at http://www.icty.org/en/action/cases/4, accessed at 20th May 2019; Parliamentary Assembly of the Council of Europe. Resolution 1670, "*Sexual violence against women in armed conflict*", adopted on 29th May 2009, para. 6, accessed at 22nd May2019.

In 1997, Radovan Karadžić was sued, by several Bosnian and Croatian women, in an American court for "genocidal rape". He was found liable, and victims of genocidal rape were awarded $ 745 million in damages.[34]

On June 26th, 1996, TPIY accused Dragan Zelenović of seven charges of rape and torture as "*crimes against humanity*" and seven charges of rape and torture as "*violations of the customs and laws of war*". Zelenović initially pleaded not guilty, but at a hearing on December 17th, 2007, the trial court accepted a plea of guilty in three torture cases and four rape cases as a "*crime against humanity*". Zelenović participated in the sexual assaults of women from different camps, including in group rape on a 15 years old girl and an adult woman. He received a 15 years sentence for "*crimes against humanity*". The Board of Appeal upheld the original thesis.[35]

On March 10th, 1997, in the best known trial under the case of Čelebići, Hazim Delić, Zejnil Delalić, Zdravko Mucić and Esad Landžo were tried. They were charged with Article 7 (1) - "*A superior may be held liable for the crimes of his subordinates, if he (a) has failed to prevent the commission of these crimes, knows or has reason to know that it is it may have been committed, or (b) it did not punish those who committed it* "and Article 7 (3) of the ICT Statute for "*violation of international humanitarian laws*". The offenses took place in camps in the Bosnian and Croatian prisons, controlled by Čelebići. Delić was found guilty of using rape as "*torture*", which was a violation of the Fourth Geneva Convention and violated the laws and customs of the war. The court also found that Mucić was guilty of crimes committed while he was the camp commander, under the principle of command responsibility, which included gender-based atrocities. "*A person who orders an action or omission with the awareness of the high probability that an offense is committed in the execution of the respective order, has the necessary obligation to establish the liability under Article 7 paragraph (1), following the given order, and regarded as accepting this*."[36]

In June 22nd, 1998, Anto Furundžija, who was detained on December 18th, 1997 by Dutch forces operating within NATO, was tried in a trial that was one of the shortest trials heard by TPIY. This was the first case heard by TPIY dealing exclusively with rape allegations. Furundžija - a Bosnian Croat, local commander of the militia known as "*Jokers*", who took part in the ethnic cleansing of the Lava Valley and which was under the command of the Defence Council of Croatia. Furundžija was charged with individual criminal liability, which included "*committing, planning, instigating and ordering*", or in other words "*supporting and complicity in the planning, preparation or execution of any offenses referred to in articles 2 and 3 of the statute of the court*". One witness, who was assaulted by Furundžija while questioning him, gave most of the testimony during this trial.[37]

She was beaten and another soldier forced her to have oral and vaginal sex while Furundžija was present. Furundžija did not act to prevent the assault, even though he was in command. His defender claimed that the witness was suffering from post-traumatic stress disorder and that he misidentified the accused. The trial court gave Furundžija two sentences of 10 and 8 years to be executed simultaneously, finding him guilty under article three, for violating the "*laws and customs of war" for torture and abuse of personal dignity, including rape*".[38]

[34] Sjoberg, Laura, Gentry, Caron E." *Mothers, Monsters, Whores: Women's Violence in Global Politics*", London/New York, Zed Books, 2007, pp.143-144, https://centreforfeministforeignpolicy.org/journal/ 2017/ 10/31/ women-in-combat-mothers-monsters-whores, accessed at 20th May 2019.

[35] Zelenović (IT-96-23/2), https://www.icty.org/en/case/zelenovic, accessed at 23rd May 2019.

[36] Mucić et al. (IT-96-21), https://www.icty.org/en/case/mucic, accessed at 23rd May 2019.

[37] Furundžija (IT-95-17/1), https://www.icty.org/en/case/furundzija, accessed at 23rd May 2019.

[38] *Furundzija Case*: The Judgement of the Trial Chamber Anto Furundzija found guilty on both charges and sentenced to 10 years in prison, Press release, The Hague, 10 December 1998 JL/PIU/372-E, https://www.icty.org/en/press/furundzija-case-judgement-trial-chamber-anto-furundzija-found-guilty-both-charges-and, accessed at 23rd May 2019.

In May 2009, Jadranko Prlić, a former prime minister of the self-proclaimed Croatian-Bosnian war state from Herzeg in Bosnia, was convicted of murder, rape and expulsion of Bosnians. He was sentenced to 25 years in prison.

Radovan Stankovič was a member of an elite paramilitary unit in Vukovar, commanded by Pero Elez. After Elez's death, Stankovič took over the leadership of the "Karaman House", which he used as a brothel. On November 14th, 2006, the domestic court in Sarajevo sued Stankovič and sentenced him to 16 years for compelling women to prostitute. On May 26th, 2007, while being transported to the hospital, Stankovič escaped custody.[39]

Neđo Samardžić was sentenced to 13 years and 4 months after being found guilty of "*crimes against humanity*". He was indicted on ten counts, of which four were found guilty. These include multiple rapes, beatings, murder and forcing women to be sex slaves. Samardžić was also found guilty of the atrocities committed at the "*Karaman House*". Samardžić appealed and received 24 years in prison, being found guilty of nine of the ten charges.[40]

Gojko Janković surrendered to the Bosnian authorities in 2005. He was transferred to The Hague for trial, but the TPIY sent him back to Bosnia for trial before the national court. He was charged with "violations of rights, concealment and complicity, issuing orders" during an attack on the non-Serb population, which led to the killing and sexual abuse of non-Serbs, most of whom were women and Bosnian girls. He was found guilty and received a 34 years in prison sentence.[41]

Dragan Damjanović, who received 24 years in prison, was convicted of "*war crimes, including crime, torture and rape".*[42]

Momir Savić received 18 years in prison in July 2009 for the crimes he committed during the command of the Serbian army "*Višegrad Brigade*". He was convicted of the repeated rape of some Bosnians, arson, robbery and execution of executions.[43]

In January 12th, 2009, Željko Lelek received 13 years in prison for "*crimes against humanity*", including rape. Lelek, who was a police officer at the time, was convicted for his actions during the Višegrad massacres.[44]

Miodrag Nikačević, a police officer from Foča, was indicted by the domestic court in 2007 for "*crimes against humanity*" in 1992. The indictment against him has filed numerous rape cases. In April 1992, Nikačević being in army robbed and forcibly raped a woman. The second charge was for the abuse and rape of another woman in July 1992 in Foča. During the trial, the defence brought in ten witnesses who claimed that Nikačević did not participate in any war crimes and that he sometimes risked his own safety to help others. He was found guilty on February 19th, 2009 and was sentenced to 8 years in prison for rape of both women and for "*concealing and complicity in abduction and unlawful detention*"[45] of a Bosnian civilian, who was later killed in a location unknown.

[39] Radovan Stankovič, CASE NO.: IT-96-23/2-I, https://www.icty.org/x/cases/stankovic/ind/en/stan-3ai031208.htm, accessed at 23rd May 2019.

[40] Nedjo Samardzic, https://trialinternational.org/latest-post/nedjo-samardzic/, accessed at 23rd May 2019.

[41] Janković, Gojko, http://www.haguejusticeportal.net/index.php?id=6076, accessed at 24th May 2019.

[42] Prosecutor's Office of Bosnia and Herzegovina v. Dragan Damjanović, Court of Bosnia and Herzegovina, Section I for War Crimes, Appellate Division, Bosnia and Herzegovina, Case numberX-KRŽ-05/51, http://www.internationalcrimesdatabase.org/Case/983/Damjanovi%C4%87-(Dragan)/, accessed at 24th May 2019.

[43] Momir Savić, "*Visegrad Genocide Memories*", https://genocideinvisegrad.wordpress.com/tag/momir-savic/, accessed at 24th May 2019.

[44] *Zeljko Lelek, Case number: X-KRŽ-06/202,* https://trialinternational.org/latest-post/zeljko-lelek/, accessed at 24th May 2019.

[45] *Miodrag Nikačević, Case number: X-KR-08/500,* http://www.worldcourts.com/wcsbih/eng/decisions/2009.02.19_Prosecutor_v_Nikacevic.pdf, accessed at 26th May 2019.

Milorad Krnojelac, Janko Janjić, Dragan Gagović and others were indicted in 1992 for "*human rights violations*" committed during the ethnic purification of Foča. The indictment included a single rape charge.[46]

Ante Kovač, who was a commander of the military police in the Defence Council of Croatia, was accused, on March 25th, 2008, of "*war crimes*" committed against Bosnians in the municipality of Vitez, in 1993. He was heard of rapes in the camps detention in the region. Kovač was removed from the rape trial, but was found guilty by another witness and he was sentenced to 9 years in prison.[47]

Veselin Vlahović, also known as "*Batko*" or "*Monster of Grbaviča*", was sentenced to 45 years in prison in March 2013, after being found guilty of more than sixty charges, including murder, rape and torture of Bosnian and Croatian civilians during the siege of Sarajevo. Vlahović's punishment was the longest, longer than Sanko Kojić's, who - earlier in 2013 - was sentenced to 43 years in prison for his role in the Srebreniča massacre.[48]

According to Margot Wallström, UN Special Representative for Sexual Violence in Conflict, only 12 of the approximately 50,000 to 60,000 cases have been prosecuted since 2010. By April 2011, TPIY has charged 93 men, 44 of whom have been charged with criminal offenses related to sexual violence.[49]

On March 9th, 2005, the War Crimes Chamber of the Criminal Court of Bosnia and Herzegovina was officially inaugurated. In the beginning, this was a hybrid court of international and national judges. Since 2009, all legal actions have been submitted to the national authorities.[50]

Conclusions

In 2009, Amnesty International published a comprehensive report "*Whose Justice? Women in Bosnia and Herzegovina are still waiting*".[51] This report highlighted how Bosnia and Herzegovina authorities have neglected their obligation to provide justice and reparations to survivors of sexual violence committed during the 1992-1995 war. It provided an in-depth analysis of the painful situation in which: survivors live many years after the war, the legislative and political measures applied in both entities and the measures that the authorities must take at different levels to ensure justice and access to reparations for women who have survived sexual violence during the war.

Between 2011 and 2012, Amnesty International visited Bosnia and Herzegovina several times to find out if the situation of war rape survivors has improved since 2009. Concluding that very few things have changed in the lives of survivors, Amnesty International decided to detail in another separate report the situation in different parts of the country.

[46] Bosnia and Hercegovina, "*A Closed, Dark Place*": Past and Present Human Rights Abuses in Foca, July 1998, https://www.hrw.org/legacy/reports98/foca/, accessed at 26th May 2019.

[47] Ante Kovač, Case No: X-KR-08/489, https://trialinternational.org/latest-post/ante-kovac/, accessed at 26th May 2019.

[48] Prosecutor's Office v. Veselin Vlahović, https://www.law.cornell.edu/women-and-justice/ resource/ prosecutor%E2%80%99s_office_v._veselin_vlahovi%C4%87, accessed at 26th May 2019.

[49] Margot Wallstrom, Special Representative of the Secretary-General on sexual violence in conflict, https://www.peacewomen.org/content/margot-wallstrom-special-representative-secretary-general-sexual-violence-conflict-0, accessed at 26th May 2019.

[50] *Prosecution's Case Studies Series*, https://www.ictj.org/sites/default/files/ICTJ-FormerYugoslavia-Domestic-Court-2008-English.pdf, accessed at 26th May 2019.

[51] Report 2009"*Whose Justice? Bosnia and Herzegovina's Women Still Waiting*", Amnesty International: http://amnesty.org/en/library/info/EUR63/006/2009/en; Report 2012 "*When everyone is silent: Reparations for survivors of wartime rape in Republic Srpska in Bosnia and Herzegovina",* http://amnesty.org/en /library/ info/ EUR63/012/2012/en, accessed at 20th May 2019.

In order for Bosnia and Herzegovina to meet its international human rights obligations, its authorities must provide war rape survivors with complete reparation, including rehabilitation.

According to the existing legal framework in Bosnia and Herzegovina, the psychological, economic and social support is provided by the social assistance institutions. In Bosnia and Herzegovina there is no central government body responsible for the social assistance system. This responsibility is exercised at the level of the entity, including through the introduction and implementation of the legislation, the allocation of resources and the provision of services. The social assistance system is organized at entity level by the Sprska Republic government and delivered through the municipal social assistance departments that provide services directly to the beneficiaries.

Within the Federation of Bosnia and Herzegovina, the legislation at least provides for the formal recognition of women who have survived war rape as civilian victims of war, which entitles them to a number of different services, while the NGO sector is actively involved in addressing it and supporting this population. However, the government of the entity of the Sprska Republic still does not recognize the needs of the survivors of the war rapes - indeed, a big problem - and therefore fails to provide adequate reparation.

It is impossible for Amnesty International to assess the number of women and girls who were raped during the war and currently living in the territory of the Sprska Republic. The authorities of the Republic of Sprska have never made a significant attempt to collect data on this population, to understand their problems and to develop policies that respond to their specific needs.

In 2017, another 21 survivors of conflict-related sexual violence received official status as civilian victims of the war, as a result of the new commissions on status recognition. The pace of justice at national level has accelerated in recent years; between 2004 and 2017, 116 cases of conflict-related sexual violence were resolved, 58 cases were opened and 128 were investigated, although these figures could be incomplete, given the cases against men who are qualified, rather, as inhuman treatment than sexual violence. Concerted efforts are needed to protect victims and witnesses of intimidation in connection with war crime processes. Regarding the prevention of stigmatization, on June 19th, 2018, to mark the International Day for the Elimination of Sexual Violence in Conflict, the Inter-Religious Council, which includes leaders of the Serbian, Orthodox, Islamic, Jewish and Catholic communities, issued an inter-confessional statement denouncing stigma survivors of sexual violence and demanding increased efforts to raise their social status. On October 4th, 2018, Bosnia and Herzegovina became the first country to adopt a national plan to mitigate stigma.[52]

Sexual violence is different from other weapons. When bombs destroy roofs, affected people take refuge in their neighbors. Even the soldiers are forced to give first aid to the wounded in the opposing camp. But victims of rape and other forms of abuse are often stigmatized and expelled from the communities in which they live. Behind sexual violence lies a treacherous tactic that seeks to make room for fear, stigmatization and psychic pressure.

In 2008, the UN officially recognized sexual violence in armed conflict as a war crime. There is an urgent need for a resolution on establishing a formal mechanism to increase accountability for sexual abuse. Also, compliance with this mechanism should be regulated and supervised. The UN should carry out missions in conflict areas, set up commissions of inquiry, gather evidence and bring cases of abuse to the International Court of Justice. It is shameful that most of the mass sexual crimes committed so far have remained unpunished.

[52] "*Sexual violence in conflict: Bosnia –Herzegovina*", Report of the Secretary-General to the Security Council (S/2018/250) issued on 16th April 2018, https://www.un.org/sexualviolenceinconflict/countries/bosnia-and-herzegovina/, accessed at 22nd May 2019.

But only a UN resolution would not come. In order to ensure peace, women will need to be better represented. It could also be a good opportunity to clean up in their own backyard, as not many women have reported acts of sexual violence committed by UN troops. Gender parity in UN peacekeeping would reduce the risks and enable women to become guardians of law, order and respect for human rights. This could be the starting point in ensuring gender equality.

Thus, the issues of women's rights and in particular the distinct needs of women and girls during repatriation, resettlement of refugee camps, rehabilitation, reintegration, as well as non-participation or insignificant participation in peace negotiations and in post-conflict reconstruction, some of the essential and constant concerns of women's organizations and several institutions at international level have been for a long time.

In this regard, previously adopted other UN Security Council Resolutions, with implications on these issues - respectively 1261 of August 25th, 1999 and 1314 of August 11th, 2000 (on children and armed conflict), as well as 1265 of September 17th, 1999 and 1296 of April 19th, 2000 (on the protection of civilians in armed conflicts).

The resolution 1325/2000 was the first formal and legal document adopted by the Security Council calling on the parties to any conflict to respect the rights of women and to support their participation in peace negotiations and post-conflict reconstruction and gives a gender perspective including the special needs of women and girls precisely during the repatriation, resettlement of refugee camps, rehabilitation, reintegration, and post-conflict reconstruction. The factors that led to its adoption were the commitments of the Beijing Declaration and Platform for Action, as well as the final document of the 36th Special Session of the UN General Assembly entitled Woman 2000: Gender Equality, Development and Peace in the 21st Century, in particular references to women and armed conflict.[53]

The issue of implementing the resolution 1325/200 at both the organizational and national levels is a permanent concern at the UN and NATO levels. In support of the implementation of this Resolution, NATO and its partners carry out concerted actions, becoming the main task of the Strategic Commands to develop guidelines at the level of NATO operations, to promote the role of women in operations and missions, as well as to improve knowledge and skills on gender issues and diversity.

Resolution 2242/2015 signals the intention of the UN Security Council to create an informal expert group on "Women, Peace and Security" to ensure coherent information on the flows of conflict impact on women; this will be achieved through regular briefings of the Security Council by civil societies.[54]

Resolution 2272/2016 highlights the critical importance of the fact that civilians, especially women and children, in camps for displaced persons and refugees must be protected from any form of abuse or exploitation; to continue efforts to increase measures in United Nations peace operations against all forms of civilian abuse and exploitation by any member of the peace operation; to ensure that within the framework of peace operations, as appropriate, it will facilitate the identification of possible abuses and mitigate the stigmatization of victims.[55]

Resolution 2467/2019 reiterates the disproportionate impact of sexual violence in armed conflict and post-conflict situations on women and girls, which is further aggravated by

[53] Resolution 1325 (2000) adopted by the Security Council at its 4213th meeting, on 31st October 2000, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF 9%7D/ WPS% 20SRES1325%20.pdf, accessed at 26th May 2019.

[54] Resolution 2242 (2015), adopted by the Security Council at its 7533rd meeting, on 13th October 2015, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_res_ 2242.pdf, accessed at 20th May 2019.

[55] Resolution 2272 (2016), adopted by the Security Council at its 7643rd meeting, on 11th March 2016, https://conduct.unmissions.org/sites/default/files/n1606925.pdf, accessed at 20th May 2019.

discrimination against them, by under-representation of women in decision-making and leadership roles, multiplied by the impact discriminatory laws, the application of gender-biased laws and harmful customs in society, on continuous and recurrent frameworks of violence against women and girls. In situations of armed conflict and post-conflict, it is essential to discourage and prevent sexual violence, by recognizing national ownership and responsibility in addressing the root causes and the consistent and rigorous pursuit of crimes of sexual violence. The need for civilian and military leaders, to demonstrate their commitment and political will to prevent sexual violence and to impose responsibility in conflict and post-conflict situations, not tolerating the fact that sexual violence in armed conflict is a cultural phenomenon or a consequence inevitable war or lesser crime. Recognizes the role of United Nations Action against Sexual Violence in Conflict as the inter-agency coordination forum chaired by the Special Representative on Sexual Violence in Conflict to address this problem, and encourages the revision and continued development of innovative operational tools and guidance by United Nations Action against Sexual Violence in Conflict.[56]

The UN Security Council resolution on rape will not bring those women's daughters back. But it is nonetheless historic because, finally, sexual violence is recognized as a weapon, and can be punished. No longer can a man defend himself by saying that he could have killed a woman he had "only" raped. We know now, as we knew even before the passage of this resolution, that *"rape is a kind of slow murder*".[57]

BIBLIOGRAPHY

1. Abu-Hamad, Aziz, "Rape as a Weapon of War", The Human Rights Watch Global Report on Women's Human Rights (PDF), Human Rights Watch, 1995.
2. Bayard, Pierre, "Collective Rape and Post memory in Bosnia", Journal of Literature and Trauma Studies 4 (2015).
3. Lončar, Mladen, Medved, Vesna, "Psychological consequences of rape on women in 1991–1995 war in Croatia and Bosnia and Herzegovina" Croatian Medical Journal 47 (2006).
4. "Bosnia-Herzegovina - Gross abuses of basic human rights" Report AI Index: EUR 63/01/92, Amnesty International October 1992.
5. Bosnia and Hercegovina, "A Closed, Dark Place": Past and Present Human Rights Abuses in Foca, July 1998.
6. Full Warburton Mission II Report, February 1993, EC Investigative Mission into the treatment of Muslim Women in the Former Yugoslavia: Report to EC Ministers.
7. "Legacies and Lessons: Sexual violence against men and boys in Sri Lanka and Bosnia & Herzegovina", UCLA School of Law: Health & Human Rights Project, All Survivors Project, 2017.
8. Parliamentary Assembly of the Council of Europe Resolution 1670 (2009), "Sexual violence against women in armed conflict", adopted on 29 May 2009, para. 6.
9. Report 2009 "Whose Justice? Bosnia and Herzegovina's Women Still Waiting", Amnesty International.
10. Report 2012 "When everyone is silent: Reparations for survivors of wartime rape in Republic Srpska in Bosnia and Herzegovina", Amnesty International.

[56] Resolution 2467 (2019), adopted by the Security Council at its 8514th meeting, on 23rd April 2019, https://undocs.org/S/RES/2467(2019), accessed at 22nd May 2019.

[57] Drakulic, Slavenka, "*They Would Never Hurt a Fly: War Criminals on Trial in The Hague*", Penguin Books; Reprint edition July 26th, 2005, p. 24.

11. Resolution 1325 (2000) adopted by the Security Council at its 4213th meeting, on 31st October 2000.
12. Resolution 2242 (2015), adopted by the Security Council at its 7533rd meeting, on 13th October 2015.
13. Resolution 2272 (2016), adopted by the Security Council at its 7643rd meeting, on 11th March 2016.
14. Resolution 2467 (2019), adopted by the Security Council at its 8514th meeting, on 23rd April 2019.
15. Security Council strongly condemns humanitarian law violations by Bosnian Serbs, Paramilitary Forces; Cities summary executions, mass expulsions, Press release SC 6149, 21st December 1995.
16. "Seventh Report on War Crimes in the Former Yugoslavia: Part II". US submission of information to the United Nations Security Council, 1993.
17. “Sexual violence in conflict: Bosnia –Herzegovina”, Report of the Secretary-General to the Security Council (S/2018/250) issued on 16th April 2018.
18. “When everyone is silent –reparation for survivors of wartime rape in Republic Srpska in Bosnia and Herzegovina”, Amnesty International Publications, 31st October 2012.
19. Allen, Beverly – “Rape Warfare: Hidden Genocide in Bosnia-Herzegovina and Croatia”, University of Minnesota Press, 1996.
20. Becirevic, Edina “Genocide on the Drina River”, New Haven, CT: Yale University Press, 2014.
21. Buss, Doris, "Prosecuting Mass Rape: Prosecutor v. Dragoljub Kunarac, Radomir Kovac and Zoran Vukovic", Feminist Legal Studies 10 (1), 2002.
22. Crowe, David M. - “Crimes, Genocide, and Justice: A Global History” Palgrave Macmillan, 2013.
23. Cohen, Philip J. - "The Complicity of Serbian Intellectuals", In Cushman, Thomas, Mestrovic, Stjepan G. (Eds.), “This Time We Knew: Western Responses to Genocide in Bosnia” New York University Press.
24. Drakulic, Slavenka, “They Would Never Hurt a Fly: War Criminals on Trial in The Hague”, Penguin Books; Reprint edition July 26th, 2005.
25. Ferguson, Niall –“The War of the World: History's Age of Hatred”, Penguin Morales, 2009.
26. Ferguson, Niall, “The War of the World: Twentieth-Century Conflict and the Descent of the West”, (Reprint ed.), Penguin, 1996.
27. Henry, Nicola -“War and Rape: Law, Memory, and Justice”, Routledge, 2010.
28. Sjoberg, Laura, Gentry, Caron E, ”Mothers, Monsters, Whores: Women's Violence in Global Politics”, London/New York, Zed Books, 2007.
29. Steven L. Burg; Paul S. Shoup – “Ethnic Conflict and International Intervention: Crisis in Bosnia-Herzegovina, 1990-93” Taylor & Francis, 2015.
30. Stiglmayer, Alexandra - "The Rapes in Bosnia-Herzegovina", in Stiglmayer, Alexandra (Ed.). Mass Rape: The War against Women in Bosnia-Herzegovina, University of Nebraska Press, 1994.
31. Tausan, Marija, "Defence Witnesses Speak about Abusers in Uzamnica", BRIN, 20th August 2013.
32. Totten, Samuel, Bartrop, Paul R, “Dictionary of Genocide”, 2007.
33. Weitzman, P.A, “The politics of identity and sexual violence: A review of Bosnia and Rwanda”, Human Rights Quarterly, 30, 2008. https://www.amnesty.org
34. https://centreforfeministforeignpolicy.org
35. https://conduct.unmissions.org

36. https://genocideinvisegrad.wordpress.com
37. http://www.haguejusticeportal.net
38. https://www.hrw.org
39. https://www.icrc.org
40. https://www.icty.org
41. https://www.ictj.org
42. http://www.internationalcrimesdatabase.org
43. https://www.law.cornell.edu
44. https://link.springer.com
45. https://www.peacewomen.org
46. https://www.reuters.com
47. https://www.securitycouncilreport.org
48. https://www.theglobeandmail.com
49. https://trialinternational.org
50. https://undocs.org
51. https://www.un.org
52. http://www.worldcourts.com

THE USE OF THE UNIFORM OF THE ENEMY — BETWEEN PERFIDY AND RUSES OF WAR

Sabin GUȚAN
Assist. Prof., The "Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania,
sabin_gutan@yahoo.com

Abstract: *International humanitarian law requires participants in the armed conflict to respect the principle of distinction, in order to differentiate themselves from civilians. The principle of distinction is transposed in practice by wearing a uniform or fixed distinctive sign recognizable at a distance. Wearing uniforms or signs of protected bodies or belonging to neutral states are prohibited by international humanitarian law, entering the sphere of perfidy and war crimes. However, wearing an opponent's uniform during armed conflicts is not always considered treachery, but only when it results in the injury or the killing of an opponent. The rest of the situations are loosely covered by the international humanitarian law, interfering with other legal institutions, such as espionage or even ruses of war. There are also situations where international humanitarian law overlaps with domestic law, as is the case of art.241 of the Romanian Criminal Code — Illegal wearing of decorations or distinctive signs.*

Keywords: *the use of the uniform of the enemy, perfidy, ruses of war, espionage, principle of distinction*.

The Regulation

There are a number of regulations regarding the use of the enemy's uniform in times of international armed conflict, both in written and customary law. Thus, Article 23 (f) of the Regulation annexed to the Fourth Hague Convention of 1907 respecting the Laws and Customs of War on Land prohibits: ”*to make improper use of a flag of truce, of the national flag or of the military insignia and uniform of the enemy, as well as the distinctive badges of the Geneva Convention*”.

Moreover, Article 39 (2) of Additional Protocol I to the Geneva Conventions of 1949, adopted in 1977 in Geneva, on the protection of victims of international armed conflicts, stipulates that: ”*It is prohibited to make use of the flags or military emblems, insignia or uniforms of adverse Parties while engaging in attacks or in order to shield, favour, protect or impede military operations*.” As far as the regulation in Article 39 (1) of Additional Protocol I ("It is prohibited to make use in an armed conflict of the flags or military emblems, insignia or uniforms of neutral or other States not Parties to the conflict.") is regarded, one can notice the fact that the use of the uniforms of neutral or non-belligerent states during armed conflict is absolutely forbidden, while the prohibition on the use of the adversary's uniforms is relative, being restricted only to the carrying out of attacks or to shielding, favouring, protecting or impeding the military operations. But these provisions cannot in any way affect the application of the existing rules applicable to espionage (Article 39 (3)).

In customary international humanitarian law there is the same rule regarding the use of the adversary's uniform: ”*Rule 62. Improper use of the flags or military emblems, insignia or uniforms of the adversary is prohibited.*” [1] The Statute of the International Criminal Court, adopted in Rome in 1998, contains a similar incrimination of this fact, in Article 8 (war crimes), point b): "(vii) Making improper use of a flag of truce, of the flag or of the military insignia and uniform of the enemy or of the United Nations, as well as of the distinctive emblems of the Geneva Conventions, resulting in death or serious personal injury".

[1] Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law,* vol.1, Cambridge University Press, New York, ediția 2009, p. 213.

Meaning of the expression ”improper use”

There is no definition in the international treaties of the concept of *improper use of the military insignia and uniform of the enemy*. There are not even examples in the respective norms, as was the case of perfidy and ruses of war. Although there are interpretations and definitions of this notion in the doctrine, in decisions of courts, in military manuals, they cannot be considered generally valid. Moreover, there are a number of differences in approach from one country to another, from one period to another. The points of view vary from a maximum restriction of the right to wear the opponent's uniform (reaching up to being allowed only for his own protection), to a punctual restriction, only to prohibit the attack, not to shield, favour, protect or impede the military operations (as in the case of Canada, which made reservation to Article 39 (2) in this regard).[2]

The use by a prisoner of war of an opponent's uniform, in an attempt to escape, without causing the death or injury of an adversary, does not violate international humanitarian law. [3] In this case, if the escaped prisoner is caught by the opponent, before the escape is successful, he is liable only to a disciplinary punishment.

Many discussions and controversies are about the idea of *infiltrating enemy lines, wearing enemy uniform,* to carry out certain missions, which don’t necessarily involve the use of force. Those who support the legality of such an action invoke the decision in the Skorzeny case[4]. Towards the end of World War II, this German officer was given the mission to infiltrate the American-controlled area, along with other German military, all equipped in American uniforms, to capture some American military objectives. The purpose of this mission was to ensure the success of the German offensive. The mission failed, and the US court in question acquitted the German military, considering that they did not violate Article 23 (f) of the Regulation annexed to the Fourth Hague Convention of 1907, but without giving adequate reasons for taking this decision. However, the actions carried out by the German military are confined to the notion of attack, which also involves the preparatory acts of an attack. Some authors consider that this decision is incorrect and does not represent the letter of the law.[5] At least at the level of the present regulations, referring to the Additional Protocol I, such a decision is no longer possible. Some authors consider that fighting while wearing the enemy's uniform is perfidy, leading to the loss of the status of combatant and of the right to be a prisoner of war.[6] However, this opinion is exaggerated, exceeding both the legal sphere of perfidy and the legal meaning of the principle of distinction set out in Article 44 of Additional Protocol I.

Furthermore, using the adversary's uniform for gathering information does not violate international humanitarian law, but the military captured under these conditions can be charged with espionage.[7]

For the purposes stipulated by Article 39 (2) of Additional Protocol I, the improper use of the military insignia and uniform of the enemy refers to the preparation and conduct of attacks (offensive or defensive military actions), but in all situations directly related to

[2] See Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law,* vol.1, Cambridge University Press, New York, 2009, pp. 215-217.

[3] Jean De Preux, *Commentary on the Additional Protocols of 8 June 1977to the Geneva Conventions of 12 August 1949*, International Committee of the Red Cross, Geneva, 1987, p. 467.

[4] Case No. 56 Trial of Otto Skorzeny and Others General Military Government Court of the U.S. Zone of Germany 18th August to 9th September, 1947.

[5] Jean De Preux, *Commentary on the Additional Protocols of 8 June 1977to the Geneva Conventions of 12 August 1949*, International Committee of the Red Cross, Geneva, 1987, p. 468.

[6] Gary D. Solis, *The Law of Armed Conflict — international humanitarian law in war*, Cambridge University Press, 2010, p. 223.

[7] FM 6-27/MCTP 11-10C**,** *The Commander's Handbook on the Law of Land Warfare***,** Department of the Army Headquarters, United States Marine Corps, 2019, pp. 2-25.

military operations. Moreover, the regulation stipulated by the Additional Protocol I no longer uses the expression ”improper use”, but clearly sets out the situations in which such use is prohibited. However, this fact does not in itself constitute a serious violation of the international humanitarian law, that is, a war crime, which also results from the way in which it was incriminated by the Statute of the International Criminal Court (it is conditioned by the cause of loss of human lives or serious injuries, intentional or by negligence.)[8] This is not an impediment for states to criminalize in their domestic criminal law the use of their uniforms by the adversary.

It is clear that the use of the opponent's uniform and insignia is illegal when the combatant in question is directly involved in the fight with the opponent. The use of the opponent's uniform to infiltrate or approach the adversary does not violate the provisions of Article 23 (f) of the annexed Regulation and could be a slight violation of Article 39 (2) of the Additional Protocol I, if, before engaging in combat, the combatant in question gives up his opponent's uniform and is equipped in his own uniform.[9]

Perfidy and the use of the uniform of the enemy

Loyalty, as a principle of international humanitarian law, as opposed to perfidy, was registered in the Hague Conventions of 1899 and 1907 and was developed in Additional Protocol I of Geneva of 1977 (Article 37). Moreover, all the norms of international humanitarian law revolve around two legal-moral principles: honour and humanity, as components of loyalty.

It should be noted that Article 23 of the Regulation annexed to the Fourth Hague Convention of 1907 is not intended for perfidy, but for the prohibition of means and methods of war, some perfidious, without making a clear delimitation of these:

”*In addition to the prohibitions provided by special Conventions, it is especially forbidden:*

(a) To employ poison or poisoned weapons;

(b) To kill or wound treacherously individuals belonging to the hostile nation or army;

(c) To kill or wound an enemy who, having laid down his arms, or having no longer means of defence, has surrendered at discretion;

(d) To declare that no quarter will be given;

(e) To employ arms, projectiles, or material calculated to cause unnecessary suffering;

(f) To make improper use of a flag of truce, of the national flag or of the military insignia and uniform of the enemy, as well as the distinctive badges of the Geneva Convention;

(g) To destroy or seize the enemy’s property, unless such destruction or seizure be imperatively demanded by the necessities of war;

(h) To declare abolished, suspended, or inadmissible in a court of law the rights and actions of the nationals of the hostile party. A belligerent is likewise forbidden to compel the nationals of the hostile party to take part in the operations of war directed against their own country, even if they were in the belligerent’s service before the commencement of the war.”

At that time perfidy had not been defined, meaning that it could be considered that banning together the unlawful wearing of the enemy's uniform and insignia, on the one hand, and of the distinctive signs of the Geneva Convention, on the other, was justified by the

[8] See Arne Willy Dahl, *ICC Statute Article 8(2)(b)(vii)*, 30 May 2017, Norway, Centre for International Law Research and Policy (CILRAP), 100 Avenue des Saisons, 1050 Brussels, Belgium, www.legal-tools.org/doc/de6ce5/.

[9] Gary D. Solis, *The Law of Armed Conflict — international humanitarian law in war,* Cambridge University Press, 2010, pp. 432-434.

existence of perfidy in both cases. However, the definition and examples of perfidy in Article 37 (1) of Additional Protocol I intentionally excluded the wearing of the enemy's uniform, creating a separate regulation, in Article 39 (2).

Article 24 of the Regulations annexed to the Fourth Hague Convention of 1907 ("*Ruses of war and the employment of measures necessary for obtaining information about the enemy and the country are considered permissible*.") suggests the possibility of a fair use of the enemy's uniform in order to obtain information about the enemy.

Article 37 (1) (Prohibition of perfidy) of Additional Protocol I provides:

"It is prohibited to kill, injure or capture an adversary by resort to perfidy. Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence, shall constitute perfidy. The following acts are examples of perfidy:

a) the feigning of an intent to negotiate under a flag of truce or of a surrender;

b) the feigning of an incapacitation by wounds or sickness;

c) the feigning of civilian, non-combatant status; and

d) the feigning of protected status by the use of signs, emblems or uniforms of the United Nations or of neutral or other States not Parties to the conflict."

In order for a deed to be considered perfidy, within the meaning of Article 37 (1), it must cumulatively have three elements:[10]

a. the existence of an international norm that confers protection (which the adversary may receive or is obliged to grant);

b. giving the opponent the false impression that he is in the legal situation to receive or grant protection;

c. the intention to deceive.

In addition to this, the prohibition of perfidy by Article 37 (1) refers only to the situations related to the conduct of hostilities, only the direct participants to the hostilities being linked to it.[11]

As it results from the content of Article 37 (1), such acts shall be considered perfidy only if they are committed for the killing, injury or capture of an adversary. The prohibition against perfidy would not prevent the mere gathering of information by undercover units disguised as civilians or even wearing the enemy's uniform.[12] This fact falls under the scope of Article 46 regarding espionage.

The purpose of perfidy is very important: to deceive the good faith of the adversary, to make him believe that he has the right to receive or the obligation to grant the protection stipulated by the rules of international law applicable to armed conflicts. Therefore, not all the facts of deception of the enemy are perfidy. Those that don't violate in any way the international law applicable in the armed conflicts are ruses of war, being considered lawful. But there are also a number of facts that violate international humanitarian law, which deceive the good faith of the adversary, but the violated norms do not fall within the scope of the protection required by Article 37 (1). This is also the case of the regulation present in Article 39 (2) — use of the enemy's uniform and insignia. This fact, although often associated with

[10] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict,* Cambridge, Cambridge University Press, 2004, p. 201.

[11] Jean De Preux, *Commentary on the Additional Protocols of 8 June 1977to the Geneva Conventions of 12 August 1949,* International Committee of the Red Cross, Geneva, 1987, p. 430.

[12] Nils Melzer, *International Humanitarian Law: A Comprehensive Introduction.* International Committee of the Red Cross: Geneva, 2016, p. 109.

perfidy, according to the definition of perfidy given by Additional Protocol I, is excluded from perfidy, but not from unlawful acts.[13]

Ruses of war

Article 37 (2) makes the distinction between perfidy, as an illegal act, and ruses of war, as the permissible means of deceiving the enemy based on insight, ingenuity, stratagem (tactic based on surprise, ambush, deception, incitement of the enemy to rebellion, etc.).

Thus, Article 37 (2) stipulates that: "*Ruses of war are not prohibited. Such ruses are acts which are intended to mislead an adversary or to induce him to act recklessly but which infringe no rule of international law applicable in armed conflict and which are not perfidious because they do not invite the confidence of an adversary with respect to protection under that law. The following are examples of such ruses: the use of camouflage, decoys, mock operations and misinformation."*

The examples are enumerative, a more comprehensive list of ruses of war can be found in various military manuals: surprise attacks, ambushes, simulated land, air or naval operations, simulation of rest or inactivity, construction of unused facilities, installation of false aerodromes , fake cannons and armored vehicles, creating imitations mine fields , arranging a small unit so that it looks like a more important unit, equipped with powerful vanguard or outposts, radio or press transmission of inaccurate information, giving the opponent false documents , operation plans, telegrams, etc. without any relation to reality, the use of the enemy's wavelengths, its telegraphic codes to transmit false instructions, imitations of parachutes or simulated supplies, moving the traffic terminals or falsifying road signs, etc.[14]

Espionage in times of armed conflict

Spies are people specially trained to clandestinely collect information about the enemy during an armed conflict. Article 29 of the Regulation annexed to the Fourth Hague Convention of 1907 states that: "*A person can only be considered a spy when, acting clandestinely or on false pretences, he obtains or endeavours to obtain information in the zone of operations of a belligerent, with the intention of communicating it to the hostile party.*

Thus, soldiers not wearing a disguise who have penetrated into the zone of operations of the hostile army, for the purpose of obtaining information, are not considered spies. Similarly, the following are not considered spies: soldiers and civilians, carrying out their mission openly, entrusted with the delivery of despatches intended either for their own army or for the enemy's army. To this class belong likewise persons sent in balloons for the purpose of carrying des patches and, generally, of maintaining communications between the different parts of an army or a territory."

The collection of information by civilians or soldiers dressed in civilian clothes, due to the fundamental protection of this category against military hostilities, should always be considered an act of espionage and, of course, an action of treachery should ensue. However, the act as such does not constitute perfidy, as defined by Article 37 (1), unless it results in the killing or injury of an adversary.

Additional Protocol I details these regulations, extending the area in which a person who collects information is considered a spy (the territory controlled by an adverse party). Article 46 stipulated that the following categories of persons and activities are assimilated to espionage:

[13] Jean De Preux, *Commentary on the Additional Protocols of 8 June 1977to the Geneva Conventions of 12 August 1949,* International Committee of the Red Cross, Geneva, 1987, p. 441.

[14] Ionel Cloşcă, Ion Suceavă, *Tratat de drept internaţional umanitar*, Bucureşti, Editura V.I.S. PRINT, 2000, pp. 178-179.

- *”A member of the armed forces of a Party to the conflict who, on behalf of that Party and in territory controlled by an adverse Party, gathers or attempts to gather information shall not be considered as engaging in espionage if, while so acting, he is in the uniform of his armed forces.”* As a result, a spy is considered not to respect the principle of distinction (distinctive insignia of the army to which he belongs, carries his arms openly).

- ”*A member of the armed forces of a Party to the conflict who is a resident of territory occupied by an adverse Party and who, on behalf of the Party on which he depends, gathers or attempts to gather information of military value within that territory shall not be considered as engaging in espionage unless he does so through an act of false pretences or deliberately in a clandestine manner. Moreover, such a resident shall not lose his right to the status of prisoner of war and may not be treated as a spy unless he is captured while engaging in espionage.”*

- *”A member of the armed forces of a Party to the conflict who is not a resident of territory occupied by an adverse Party and who has engaged in espionage in that territory shall not lose his right to the status of prisoner of war and may not be treated as a spy unless he is captured before he has rejoined the armed forces to which he belongs.”* In this sense, the quality of spy exists only during the course of the respective actions in the territory occupied by the enemy.

With respect to the Regulation annexed to the Fourth Hague Convention of 1907, Article 46 of the Additional Protocol I of 1977 refers only to the members of the armed forces, and not to the civilians to whom the national law of the captive state will apply.

If a person, known to have carried out espionage activities in the past, falls into the hands of the opposing party after returning to the armed forces to which she/he belongs, she/he becomes a prisoner of war. The quality of spy is assigned only during the espionage mission and until the moment of returning to the territory controlled by the party to which she/he belongs. The spy does not benefit from the protection of international humanitarian law. However, not being a (lawful) combatant, the spy will be assimilated to the civilian population and will benefit from the protection of the Fourth Geneva Convention of 1949 and Article 75 of the Additional Protocol I. In this regard, he/she will benefit, in the case of capture, of a guarantee, respectively of a preliminary judgment in accordance with the laws of the captive state.[15]

Espionage is not considered a war crime and is not prohibited by international humanitarian law. The spy only loses his status as a lawful combatant and the right to be a prisoner of war when he/she is captured in action.[16] This is the reason for the regulation in Article 39 (3): ”*Nothing in this Article or in Article 37, paragraph 1 d), shall affect the existing generally recognized rules of international law applicable to espionage or to the use of flags in the conduct of armed conflict at sea.*” Even if the spy uses the adversary's uniform and insignia in his/her intelligence gathering actions, he/she remains bound by the espionage regulations.

Applying the criminal rules of the national criminal law

Although in times of armed conflict the rules of international humanitarian law apply, states have the possibility of applying the rules of national law. However, in case of war crimes, international treaties do not have a criminal component; they only name the facts that constitute serious violations or war crimes. The regulation and sanctioning of these crimes remains the responsibility of the states and of the international courts.

[15] Ionel Cloşcă, Ion Suceavă, *Tratat de drept internaţional umanitar*, Bucureşti, Editura V.I.S. PRINT, 2000, p.144.

[16] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict,* Cambridge, Cambridge University Press, 2004, pp. 210-211.

As far as the illegal port of military uniforms and insignia is concerned, in the Romanian Criminal Code there is a regulation in Article 241, entitled *Illegal wearing of decorations or distinctive signs,* having the following content: ”*The wearing, without right, of decorations, uniforms or distinctive signs of a state body, is punished by imprisonment from one month to 3 months or with a fine.*

The wearing, without right, of military uniforms, grades or insignia, is punishable by imprisonment from 3 months to 2 years or with a fine.

If the act provided for in the preceding paragraph is committed in time of war, the punishment shall be imprisonment from one to five years.”

The legislator considered the wearing without right of uniforms, decorations or military insignia an aggravating circumstance, and the degree of social danger is even higher if their wearing is done in time of armed conflict.

As a special legal object of the crime, we mention the social relations related to the proper wearing of the decorations, uniforms or distinctive signs of the organs of the state only by the persons to whom this right is granted, in our case, the members of the armed forces, as defined by Article 43 of Additional Protocol I.

Any person can be an active subject of the crime, the law not requiring any special quality in this regard. Thus, during the war, the deed can be committed, on the territory of the Romanian state, by an enemy as a foreign citizen. It is enough for a person to wear the uniform without right for the deed to be a crime, but we consider that the mere illegal wearing of the enemy's uniform during armed conflict cannot be considered a war crime. Committing acts of hostility by wearing the enemy's uniform can be a war crime, especially when it results in the killing or injuring of a person.

Conclusions

The use of the enemy's uniform and insignia has been part of the means and methods of warfare since ancient times. In customary law, a series of rules limiting this practice have emerged. Military honor imposes the principles of honest fighting, separating the actions of deceiving the adversary into perfidy (not allowed) and ruses of war (allowed). However, the principle of humanity further restricts this practice, by placing the use of enemy's uniform and insignia outside perfidy, but within the sphere of war crimes.

At present, there are plenty of doubts and controversy regarding the use of this method of warfare. Moreover, the prohibition in Article 39 (2) of Additional Protocol I also generated the refusal of some states to sign this document and others made reservations to this article. Many states have preferred to remain bound only by the regulation in Article 23 (f) of the Regulation annexed to the Fourth Hague Convention of 1907, which incriminates only the ”improper use”, without defining this notion.

Certainly, the fact that wearing the enemy’s uniform when in direct combat with him is an illegal act; killing or injuring an opponent in this context constitutes a war crime. The consequences of wearing the enemy's uniform without producing this result are unclear. Some of these situations may be covered by espionage; others may even be considered ruses of war.

As far as the observance of the principle of distinction, found in Article 44 of the Additional Protocol I, is regarded, we consider that this does not apply to the present situation, the principle of distinction imposing the differentiation between combatants and civilians, but not between the combatants of the two parties. Therefore, we consider that the loss of the quality of combatant and of the right to be a prisoner of war for the illegal wearing of the enemy's uniform cannot happen by invoking Article 44. Many actions in this sphere remain in the so-called gray area, between legality and illegality, many such facts remaining to the discretion of the courts that will judge them.

BIBLIOGRAPHY

1. *** Case No. 56 Trial of Otto Skorzeny and Others General Military Government Court of the U.S. Zone of Germany 18th August to 9th September, 1947.
2. *** FM 6-27/MCTP 11-10C**,** *The Commander's Handbook on the Law of Land Warfare*, Department of the Army Headquarters, United States Marine Corps, 2019.
3. Cloşcă, Ionel and Suceavă, Ion, *Tratat de drept internaţional umanitar*, Bucureşti, Editura V.I.S. PRINT, 2000.
4. Dahl, Arne Willy, *ICC Statute Article 8(2)(b)(vii)*, 30 May 2017, Norway, Centre for International Law Research and Policy (CILRAP), 100 Avenue des Saisons, 1050 Brussels, Belgium, www.legal-tools.org/doc/de6ce5/.
5. De Preux, Jean, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, International Committee of the Red Cross, Geneva, 1987.
6. Dinstein, Yoram, *The Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge, Cambridge University Press, 2004.
7. Henckaerts, Jean-Marie and Doswald-Beck, Louise, *Customary International Humanitarian Law*, vol.1, Cambridge University Press, New York, edition 2009.
8. Melzer, Nils, *International Humanitarian Law: A Comprehensive Introduction.* International Committee of the Red Cross: Geneva, 2016.
9. Solis, Gary D., *The Law of Armed Conflict - international humanitarian law in war*, Cambridge University Press, 2010.

FEW REFERENCES REGARDING THE LEGAL DIMENSION OF THE ARMS RACE IN THE CYBER ENVIRONMENT

Andra Denise ZORILĂ
Phd. candidate, Titu Maiorescu University,
avocatandrazorila@gmail.com

Abstract: *The most powerful states in the world are forced to face threats in the virtual environment in the era of cyber warfare. When analyzing the attacks / offensive operations of cyber warfare, the damages that such actions produce, according to the specialists, can be comparable to those produced by classic military operations. Currently, there are no international norms, in the field of cyber security and the arms race, to govern international conflicts in cyberspace thinking that the difficulty of creating and implementing public international rules causes a series of cyberwar actions that have happened in the last years cannot be sanctioned. This paper investigates the emergence of a dynamic arms race internationally cyber domain and we propose to highlight certain elements cyber regarding the concept of cyber warfare and the threats in cyberspace, as well as about the current evolution of the arms race in the cyber environment.*

Keywords: *arms race, cyber warfare, arms race, cybersecurity, cyberspace, cyber-arm race.*

Introduction

One of the fundamental characteristics of the confrontation between East and West during the Cold War was the arms race, a phenomenon which, with certain exceptions, covered the whole period between 1947-1989. "*The Cold War period succeeds in transforming to a considerable extent the nature of the power balance, which is now becoming a fierce arms race between the two systemic poles, doubled by an expansionary foreign policy."*[1] Although the period to which we refer, for more than four decades, has recorded the greatest increases that mankind has experienced during its existence in the field of weapons arsenals of all categories, however, from the point of view of international law have been recorded a series of progresses that regulated important aspects regarding the stagnation of the arms race. In this regard, with the active participation of the two great powers, the US and the Soviet Union, but also with the involvement of the United Nations, starting with the middle of the Cold War period, a series of international treaties were negotiated and signed that regulated the various fields of arms production and weapons of mass destruction, in this way important steps being taken towards stopping the arms race. The assessment of the specialist in public international law Gyula Fábián, referring to the danger posed by the nuclear arsenals held by some states, is extremely suggestive: *"the constant accumulation and development of weapons is similar to a person sitting on a barrel with gunpowder, having in hand a lit matchstick. States that have already accumulated a nuclear arsenal have begun to realize the negative consequences of arming in the late 1960s."*[2]

The most significant international regulations regarding the arms race were made, in the form of bilateral treaties between the two great powers, the US and the Soviet Union, but in order to give maximum force to the regulations of this extremely important area of law. International public were engaged a large number of states for the elaboration of other treaties circumscribed to stop the arms race. It is worth mentioning in this context a number of international treaties adopted during this period, with a considerable impact on the arms race,

[1] Andrei Miroiu, Simona Soare, *Balanţa de putere,* chapter included in *Manual de relaţii internaţionale,* coord. Andrei Miroiu and Radu Sebastian Ungureanu, Editura Polirom, Iaşi, 2006, p.207.

[2] Gyula Fábián, *Drept internaţional public. Note de curs*, Editura Hamangiu, Bucureşti, 2019, p.204.

regionally and globally: the 1963 Treaty on the Prohibition of Nuclear Weapons Experiments in the Atmosphere, in the Cosmic Space and Under the Water; Treaty on the Non-proliferation of Nuclear Weapons-NPT, signed in 1968; Strategic Arms Limitation Treaty (SALT -I), signed in 1972; The Missle Antiballistic Treaty - ABM, signed 1972; Biological and Toxine Weapons Convention - BTWC, was opened for signature in 1972 and entered into force in 1975, the Intermediate-Range Nuclear Forces Treaty (INF), signed in 1987 between the US and USSR etc.

After the end of the Cold War, for more than a decade, the arms race is no longer a major theme for public international law, as the US single-power status in the international system has stopped, for a moment, the ambitions of other state actors of global politics to continue. the arms race from the previous period. During the first decade of the post-Cold War period, on the line of public international law, international regulations were continued in order to prevent states from engaging in a new arms race. In this regard, a number of international treaties and conventions have been developed and signed, namely: Strategic Arm Reduction Treaty - START I, signed in 1991 between the US and USSR; Strategic Arm Reduction Treaty - START II, signed in 1993; The Open-Sky Agreement, signed in 1992; The Comprehensive Nuclear - Test-Ban Treaty - CTBT, drafted in 1996 on the basis of the UN General Assembly, has not yet entered into force; The Chemical Weapons Convention (CWC) signed in 1993 and entered into force in 1997; the Ottawa Convention signed in 1997 prohibits the use, storage, manufacture and transfer of anti-personnel mines; Arms Trade Treaty (ATT) entered into force on 24 December 2014 etc.

Although there were important international regulations in the first decade and a half after the Cold War, where it was thought that another arms race was no longer possible, a series of international events of high impact in international politics (First Gulf War, The Yugoslav Wars, the war in Iraq, the Afghanistan war, the emergence of North Korea as a nuclear power, the US withdrawal of the ABM Treaty, the war from Georgia, annexation of Crimea by the Russian Federation, the withdrawal from INF treaty) have made, according to the opinions of some reputed specialists in public international law, humanity to enter a new arms race.[3] This new arms race, unlike the Cold War period, given the spectacular advances in the field of cutting-edge technologies and cosmic space researches, will be technically superior compared to the previous one. If in the 1990s the US carried out military operations in different areas of the world, this has required very large consumption of resources related to military operations (equipment, weapons, fighting technique, etc.) and financial, at the same time Russia and the states that have detached from the former USSR drastically reduced military spending. But after President Vladimir Putin came to power, "*from 2004 Russia has intensified its military activities, carrying out the largest maritime exercise in the last 20 years and beginning to test new missile systems in response to the US withdrawal from the ABM Treaty.*[4]" We will attempt in a relatively short paper to highlight some theoretical aspects regarding the concept of the arms race, in general, and that of the arms race in cyberspace, in particular. Also, we will try to present, briefly, a number of aspects of public international law regarding the field of aggression in the cyber environment, as well as those concerning the arms race in the cyber environment.

[3] There are different opinions about the starting moment of the current arms race. Studying the specialized literature, we consider that the crucial events that contributed to the launch of the current arms race are the annexation by the Russian Federation of Crimea, in 2014 and the denunciation of the INF Treaty by the US and the Russian Federation, in 2019.

[4] Joshua S. Goldstein şi Jon C. Pevehouse, *Relaţii Internaţionale*, Editura Polirom, Iaşi, 2008, p.293.

Some considerations regarding the concept of the arms race

The concept of "arms race" presents a certain difficulty in terms of its definition. The definition of the term by authors from very diverse fields (history, sociology, military studies, strategic studies, mathematical models, political science, legal sciences, international relations, etc.) leads to the conclusion that a complete picture of the concept of "arms race" it can be achieved through a multidisciplinary approach. Some definitions of this concept, which we have identified in dictionaries, in studies of public international law and international realities, are presented below.

Various authors have noted that the process of the arms race can involve states, but also coalitions of states, which makes the "race" to acquire ever larger dimensions, both quantitative and qualitative.Thus, it is known that during the Cold War the two rival military blocs, NATO and the Warsaw Treaty, were in fierce competition in the field of arms race. Addressing the issue of state entities participating in the arms race, the author Constantin Băhnăreanu, considers the states, individually, but also the coalitions of states as the main actors in defining the arms race. Thus, the arms race is defined as "the competitive and dynamic process, constrained by the available resources, by interaction between two states or coalitions of states in the purchase of weapons".[5]

According to Joshua S. Goldstein and Jon C. Pevehouse, specialists in the field of international relations "the arms race is a mutual process in which two or more states build their military capabilities as a response. Since everyone wants to act cautiously against a threat (often a bit exaggerated in the perception of leaders), trying to respond in a form of reciprocity leads to a rush of arms production on both sides."[6] Also, American professors Michael D. Intriligator and Dagobert L. Brito, specialists in political science, defined the arms race two decades ago ”*as the competitive, resource-constrained, dynamic process of interaction between two states or coalitions of states in their acquisition of weapons".*[7]

The Encyclopedia of International Relations published in 2017 addresses the process of the arms race from the perspective of state actors who engage in such a "competition", but also of sub-state entities that, on a smaller scale, can engage in such a race:” The arms race did not exist only between states and / or coalitions of states, but also within a state, there can be processes of arming groups with their own and opposite objectives in relation to the respective state”.[8] The International Security Dictionary also states that *"the arms race takes place when two or more parties rapidly increase their military capabilities, both qualitatively and quantitatively, in response to similar increases by the other party (...) This explanation of the arms race places its causes in the external competition. Some analysts dispute this fact and argue that the roots are in the domestic politics and that these arms races happen when the interests of the military-industrial complex exert too much influence on the institutions that decide the policies. Regardless of the reasons, increasing the military capacity of a state is not, on its own, an arms race. There must be two or more parties acting in a rising spiral in order to talk about the arms race."*[9]

How can we explain the fact that states engage in extremely expensive arms races? The "security dilemma" is a concept used especially in the field of international relations to explain why the arms races are triggered and to clarify the motivations for producing the arms races known by human history. According to the realistic school of international relations, by

[5] Constantin Băhnăreanu, *Cursa înarmărilor în arcul de insecuritate din vecinătatea estică a Uniunii europene. Consecinţe pentru România*, Editura Universităţii Naţionale de Apărare ”Carol I”, Bucureşti, 2010, p.8.

[6] Joshua S. Goldstein şi Jon C. Pevehouse, *Op.Cit.*, p. 110.

[7] Michael D.Intriligator şi Dagobert L. Brito, *Arm races, Defence and Peace Economics*, February 2000, Vol 11, accessed January 23, 2020, on https://www.ruf.rice.edu/~econ/papers/1999papers/01Brito.pdf.

[8] Dan Dungaciu (coord), *Enciclopedia relaţiilor internaţionale, Vol.I*, Editura Rao, Bucureşti, 2017, p.276.

[9] Paul Robinson, *Dicţionar de securitate internaţională*, Editura CA Publishing, Cluj Napoca, 2010, pp. 69-70.

the way states position themselves and act within the international system, the "security dilemma" is born, a concept that means that by the actions they take to strengthen their security, it's affected the security of other states.[10] In other words, increasing the military power of a state by accumulating more and more efficient weapon systems means at the same time a decrease in the military power of rival states which, in turn, are obliged to respond with weapons measures. Thus, the security dilemma is a major cause of arms races, an action that involves huge consumption of financial resources for the production/procurement of weapons with which states threaten each other, but this doesn't provide those states the security they wanted.[11]

One of the common theoretical approaches to the arms race also concerns its consequences on the international environment in general, and on relations between states in particular. As it is known, studying the period when humanity was confronted with the phenomenon of the arms race, it was found that the arms race exacerbated the tensions between states, increasing the possibility of armed conflicts at regional or even global level. Also, the arms race, through the risks that it develops with the accumulation of quantities of weapons and military technique, increases the probability of an accidental war outbreak. Arms courses, either they develop to a regional level or with the participation of the great powers capable of acting to a global level, erode the relations between the states and make the probability of the outbreak of wars increasing. Theoretical studies on the arms race, for the most part, highlight its negative role, but many authors in the field of international relations shows that *”the arms race can increase the security and prevent the war by providing a credible element of discouragement by each side”*.[12] The authors who support the thesis of a low probability of war on the background of an arms race offers as an example the competition in the domain of nuclear weapons during the Cold War between the US and Soviet Union. The strategic balance between the two superpowers, which lasted over four decades, is known in the literature as the "balance of terror" that beyond a few dangerous crises between West and East, has managed to avoid a direct armed confrontation between the USA and the USSR.

Currently, more than three decades after the fall of the Berlin Wall, after one decade and a half "apparent pause", humanity is experiencing a new arms race, with developments in various fields necessary for military operations, but also in non-military sectors, that can cause comparable damages to those produced by classic military actions. Theoretical approaches to the current arms race often make quantitative and qualitative comparations with the arms race during the Cold War. But the spectacular progress into the science area, cutting-edge technologies, and artificial intelligence applied in the domain of armaments construction systems, ammunition and various categories of military technique, makes the current arms race a completely new process, with a strong geopolitical impact to many regions, but also on a global scale. *”The arms races in the twenty-first century will be very different from the Cold War arms race. One of the things that is different about arms races now is the presence of increasing returns in the production of weapons. Further, the presence of increasing returns to scale in production is reinforced by the fact that software, microelectronics, and information are becoming increasingly important components of modern weapons systems. A thirty-year old airframe with modern electronics, software, and computers can dominate a modern airframe with antiquated equipment”*.[13]

Even if a global arms race between the great powers was not recorded, during the first decade and half after the end of the Cold War, numerous statistical data concerning the

[10] John Herz, *Idealist internationalism and the security dilemma*, World Politics, 2 (2). 1950, pp.157-180.
[11] Joshua S. Goldstein şi Jon C. Pevehouse, *Op.Cit.*, pp.119-120.
[12] *Ibidem,* p.70.
[13] Michael D.Intriligator şi Dagobert L. Brito, *Op.Cit.*

production and sale of weapons systems, ammunition and fighting techniques shows that the mankind deals, during all this period, several arms races, in different regions, by all continents. Thus, the arms race between Israel and several Arab countries in the Middle East continued, both quantitatively and qualitatively, a process that included the acquisition of both last-generation weapons and military technique. Also in this region, the United States has developed important arms sales contracts with Saudi Arabia, based on cutting-edge technology, and has delivered missile defence systems to Israel. The nuclear arms race between India and Pakistan, two rival neighboring countries continued and both states wanted to demonstrate that they represent nuclear forces, conducting nuclear tests in 1998, violating the norms of international law. Also, North Korea, which began to develop its nuclear program for military purposes since the 1990s, withdrew in 2003 from the Nuclear Non-Proliferation Treaty (NPT), so that in 2005, over three years, to test its first low-power nuclear charge. Currently, although several stages of negotiations[14] with Phenian have been completed for ending the North Korean nuclear program, even so, the communist regime has made significant progresses for designing and manufacturing ballistic missiles, managing to get intercontinental ballistic missiles with a radius of approx. 10.000 km, which caused a real concern from the United States, but also from the countries in the East Asia region. North Korea's aggressive behavior, based on its ambitious nuclear weapons program, is one of the major causes that has generated a very dynamic arms race in recent years in the East Asia region. But apart from the mentioned regions, where there have been arms races, there are other regions of the world where such processes take place, but we do not intend to develop this topic in this study.

Regarding the arms race in the cyberspace, we would like to mention that, although we have not noticed official statements by the states about the progress of this process, there are a number of studies on the militarization of the cyberspace as well as articles in the media that argue, arguably, about a real arms race and cyberspace. *"Media reports frequently use the term 'arms race' to describe the global proliferation of cyber warfare capabilities as states respond to their security concerns."*[15] In relation to other areas, especially those concerning the military security of the states, we believe that the concept of "cyber warfare capabilities" is essential for defining and evaluating the arms race in cyberspace, in order to be able to quantitatively evaluate these technologies, as well as the pace of their production. Also, apart from the "quantitative" dimension of the process, is extremely important the qualitative dimension of cyber warfare capabilities, both offensive and defensive cyber weapons.

The existence of an arms race in the cyberspace, even though it is not a priority topic on the daily agenda of specialized institutions in the field of security, has been confirmed by a number of cybersecurity specialists and a series of opinion polls: *"For 57% of security experts and policy elites, the cyber arms race is a reality according to a 2012 survey"*[16]. However, although it is recognized by a number of specialists in security studies as "part" of the general arms race, the arms race in cyberspace remains a difficult process to evaluate, as it is difficult to establish the capacity of cyber warfare for each state in this area.

[14] Since 1992 were periods when the Phenian has accepted inspections from the International Atomic Energy Agency (IAEA). In 2003, negotiations were held on the topic of the Phenian nuclear program, with the participation of the US, China, Russia, Japan, South Korea and North Korea. Also, in 2012 the Obama administration signed an agreement with North Korea to stop nuclear tests and ballistic missile launches. In 2018-2019 the leaders of the US and North Korea, Donald Trump and Kim Jong Un, met three times, but negotiations on the Phenian nuclear program and arsenal did not end with spectacular results.

[15] Gordon Corera, *Rapid escalation of the cyber-arms race*, BBC News, 29 April 2015, accessed January 13, 2020, on http://www.bbc.co.uk/ news/uk-32493516.

[16] Anthony Craig and Brandon Valeriano, *Conceptualising cyber arms races*, 2016 8th International Conference on Cyber Conflict, 2016 © NATO CCD COE Publications, Tallinn, p.142, accessed January 8, 2020, on https://www.researchgate.net/publication/305871947_Conceptualising_cyber_arms_races.

Considerations about cyberspace, cyber-attacks and international regulations of the arms race in cyberspace

As we presented in the first part of this study, the current arms race, as a whole, is very different from that of the Cold War period. Thinking to the unimaginable qualitative progress achieved today by the construction of various weapon systems, combat technique and ammunition used in combat, the current arms race has expanded to other areas such as cyberspace, about only few could imagined before of the Berlin Wall fall, that it will become a true "field" of military and non-military actions, but also a "confrontation ground" of the states of the world. We will briefly refer to some aspects of the arms race in the cyber space, a process where, next to the great powers of today's world, more and more state actors from different parts of the world have started to get involved, amidst the connection of states, almost in their entirety, on global communications networks. Outside some theoretical problems regarding the arms race in the cyberspace, we will present some aspects circumscribed to the public international law regarding the current arms race in the cyber space.

This study is based on the hypothesis supported by many cyber security specialists that the current arms race is also taking place in the cyberspace, given the increasing tendency in the last two decades of militarization of this space. We do not intend to bring scientific arguments to verify this hypothesis, this aspect being within the reach of cyberspace security experts, but we will consider highlighting a number of legal issues, from recent years, circumscribed to public international law, which are intended to counteract the aggression in the cyber environment and stop the arms race in the cyberspace.

Along with land, sea, air and space, the territories where armed confrontations have traditionally taken place, cyberspace has become the fifth area of conflict where, although the confrontations do not have the violence of those in the real area of military operations, the effects that the operations produce from the cyberspace they can sometimes be comparable to those from the real space of the armed confrontations. Whether we are considering armed clashes between states that have taken place in recent years, or whether we refer to hybrid warfare actions by certain states, cyber attacks have not been lacking in the arsenal of non-violent means used especially by the state actors that triggered them, the respective operations. *”The last few years have witnessed a proliferation of headline-grabbing cyberattacks perpetrated both by organized crime groups seeking financial gain, as well as nation-states who are increasingly using cyber-attacks as means to extend their geopolitical reach”.*[17]

The increasing number of cyber attacks on information networks and systems in recent years[18], but especially the very large damage that these attacks have caused to some states, has made these forms of cyber aggression to be included by the experts in security and international law specialists on the list of elements concerning international peace and security. The multiplication of cyber attacks, on those information systems belonging to the cyberspace, is one of the essential reasons that determined the states, but also a number of

[17] Cristian Barbieri. Jean-Pierre Dernis and Carolina Polito, *Non-proliferation Regime for Cyber Weapons. A tentative study*, Instituto Affari Internazionali (IAI), Documenti IAI18/03-March 2018, accessed January 9, 2020, on http://www.iai.it/sites/default/files/iai1803.pdf.

[18] The cyber warfare literature often refers to Russia's cyber war against Georgia in 2008, for multiplying the effect of the military operations carried out by the Russian armed forces against the Georgians. This war of Moscow has aimed "denial of service" attacks targeting sites of Georgia's government institutions, media institutions, banks and financial institutions as well as other public and private entities. . The site of Georgian President Mihail Saakaşvill was also attacked. Also, often in the scientific studies from recent years concerning the concept of cyber warfare, also refers to Russia's cyber attack on Estonia, in 2007, an event that the Estonian authorities claimed to NATO and succeeded to introduce the cyber attack into the threats chapter to the security of the Alliance state.

international institutions, to approach more and more seriously the problem of implementing international law regulations that will stop the cyber war actions, but also the arms race in cyberspace. The desire of states to achieve a fair and equitable governance in the cyber environment achieving to eliminate any illicit activity, but also to avoid the huge damage that cyber war actions can produce to the states and private entities, have generated initiatives and actions from the states, on the line of public international law, for finding rules for managing the cyberspace. The involvement of Russia in the last US presidential elections in 2016, using actions specific to the cyber war, but also in the election campaigns in other states, is an edifying example that demonstrates the urgent need to develop international law regulations that counteract cyber war actions: *”A Department of Homeland Security report, in 2019, confirms that in 2016, Russia most likely conducted research and reconnaissance against election networks in all 50 states. They breached and extracted data from one state registration database, used spear-phishing attacks to gain access to and infect computers at a voting technology company, and successfully breached election networks in at least two Florida counties. The very infrastructure that allows Americans to vote was under attack”.* [19]

The difficulty of reaching an international agreement on cyberspace, which also concerns the arms race in this area, derives from the fact that a number of important concepts such as "cybersecurity" and "cyberspace" are defined differently by the main state actors. which have the greatest influence in the cyber environment. Thus, the US defines "cyber space" as "a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controller"[20]. Other states have a different definition than Washington's about the cyber environment and cybersecurity. The government of the Russian Federation defines cybersecurity as an information security and cyberspace as an "information space". Also, few are the cyber experts who currently consider China as the largest power acting in this environment, the United States over the last few years giving the leadership of the cyber environment to the power of Beijing. However, the principle of cyber sovereignty promoted by China is in contradiction with that of an open Internet, promoted by the US state.

First of all we need to define exactly what constitutes a cyber attack. Once cyber attack is defined, what customary international law applies and to what extent? Does a cyber attack constitute a threat or use of force as outlined by the U.N. Charter, and, if so, when does a cyber attack escalate to the point at which a nation can retaliate while claiming self-defence? In his book Cyber War, Richard Clarke defined "cyber warfare" as: *”The unauthorized penetration by, on behalf of, or in support of, a government into another nation's computer or network, or any other activity affecting a computer system, in which the purpose is to add, alter, or falsify data, or cause the disruption of or damage to a computer, or network device, or the objects a computer system controls”.* [21]

One of the important principles in international law is the prohibition of the use of force. It is anchored in Article 2(4) of the UN Charter, and is considered, as ruled by the

[19] Lawrence Norden and Daniel I. Weiner, *US election are still not safe from atack. Congress can change that it if acts fast*, Foreign Affair, July 23, 2019, accessed January 23, 2020, on https://www.foreignaffairs.com/articles/russia-fsu/2019-07-23/us-elections-are-still-not-safe-attack?utm_medium=newsletters&utm_source=fatoday&utm_content=20190723&utm_campaign=FA%20Today%20072319%20U.S.%20Election%20Security%2C%20Brexit%20and%20British-EU%20Ties%2C%20Tensions%20in%20the%20Strait%20of%20Hormuz&utm_term=FA%20Today%20-%20112017.

[20] Richard Kissel (ed.), *Glossary of Key Information Security Terms*, in NIST Interagency/Internal Report (NISTIR), No. 7298rev2 (May 2013), p. 58, accessed January 19, 2020, on https://www.nist.gov/node/579721.

[21] Richard Clarke, *Cyber War: The Next Threat to National Security and What to Do About It***,** Paperback – April 10, 2012, p. 145.

International Court in The Hague, one of the Charter's cornerstones.[22] Article 2(4) states, "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." If force is used against a state, there are liable to be far-reaching consequences. When the use of force is sufficiently grave, and considered an 'armed attack,' the attacked state has the right to make counter-use of force in self-defence.[23] Do these principles and rules, which came into being with regard to the use of conventional, kinetic, weapons, also apply to the use of 'weapons' such as computers and communications networks? The common opinion is yes. The International Court in The Hague ruled that the prohibition on the use of force applies to any and every use of force no matter what type of weapon is used. The dominant position in the West is that a cyberattack will amount to an armed attack if its characteristics and consequences resemble a kinetic armed attack.[24]

The arms race in cyberspace, even if it is not officially recognized by the great powers of today's world, is a process that is unfolding rapidly and which engages an increasing number of states of the world. "Some reports estimate that around 30 countries have offensive cyber capabilities, however, those developing capabilities covertly are likely to be much higher"[25]. Although there is no unitary opinion in international law regarding the different terminology used by states regarding the militarization of cyberspace (different definition of concepts such as "cyberspace", "cyberwar", "cyber attack", "cyber conflict", "actions cyber warfare "," cyber warfare capabilities ", etc.), the efforts made by a number of specialists in public international law after the "events" in Estonia and Georgia, over a decade ago, led to a series of positive results, in the direction of the international legal framework targeting the cyberwar and the arms race in the cyberspace. Thus, the NATO Cyber Defence Center of Excellence, established in Tallinn in 2008, has elaborated the Tallinn Manual (considered by many experts as "the most comprehensive analysis of how existing international law applies to cyberspace".[26]

Defining by the Tallinn Manual of cyberspace is an important step in the direction of its legal regulation, is based on principles specific to international law. Thus, the permanent intersection, in recent years, of cyberspace with the field of international security is, perhaps, the most powerful reason for the necessity of defining the concept of cyberspace: *"The environment formed by physical and non-physical components to store, modify, and exchange data using computer networks".[27]* This definition, compared to other previous definitions, delimits the cyberspace very well, specifying that it also has a physical "dimension" represented by computers, which are located in a space belonging to a certain state. The acceptance by states of this definition of cyberspace (a union between a physical and a non-physical dimension) is of particular importance because it leads to the idea that an international legal regime regarding the management of cyberspace can be established.

[22] Frank J. Cilluffo, Sharon L. Cardash, and George C. Salmoiraghi, *A Blueprint for Cyber Deterrence: Building Stability through Strength*, Military and Strategic Affairs 4, No. 3 (December 2012).

[23] Article 51 of the UN charter states that: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."

[24] Sheng Li, *When Does Internet Denial trigger the Right of Armed Self-Defence*?, 38(1) Yale Journal of International Law (November 15, 2012), p. 200.

[25] James R. Clapper, Marcel Lettre and Michael S. Rogers, *Foreign Cyber Threats to the United States*, Joint Statement for the Record to the Senate Armed Services Committee, 5 January 2017, accessed January 29, 2020, on https:// www.armed-services.senate.gov/download/clapper-lettre-rogers_01-05-17.

[26] *Atlantic Council, International Law and Cyber Operations - Launch of the Tallinn Manual 2.0*, Washington, 8 February 2017, accessed January 28, 2020, on http://www.atlanticcouncil.org/events/detail/international-law-andcyber-operations-launch-of-the-tallinn-manual-20.

[27] Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Cambridge, Cambridge University Press, 2017, p. 564.

Concerns over the definition of cyberspace and cyberwar have been noted in the last decade and outside the community of Western states. Thus, in 2011, Russia proposed within the Shanghai Cooperation Organization to define terms (cyberspace, cyberwar, information space, information war), finding major differences compared to the vision of Western powers. The draft Convention on International Information proposed by Russia, on that occasion, highlighted the difference of vision between Moscow and the West on the definition of cyberspace, but also on the concept of information war, differences that have made the US and other states. Europeans to reject the draft convention desired by Moscow.

Given China's ascendancy in current world politics, China's publicly expressed desire to become a cyber-superpower, it is important to clarify a number of issues regarding the Chinese state's cyberspace policy. Thus, since 2013, Chinese diplomats have accepted that international law and the UN Charter apply in cyberspace, and they have agreed with four norms of states behavior - neutrality, proportionality, the right to self-defence and the fact that other concepts of international law would it could be applied to conflicts in cyberspace.[28] Also, in this context, we must point out that the principle of cyber sovereignty, promoted by Beijing, is in contradiction with the principle of open Internet promoted by the US.

An important moment in the direction of the urgency of the elaboration of international regulations regarding the arms race and the cyberwar was the declaration of NATO leaders states, at the Warsaw Summit of July 2016, specifying that *"cyberattacks present a clear challenge to address of Alliance security and could be just as damaging to modern societies as conventional attacks."*[29] The statement confirms that threats from the cyberspace can no longer be disregarded and urges NATO and allied states management structures to develop strategies to counteract cyberwar actions, while at the same time continuing to create the international legal framework that will regulate, as clearly as possible, the problem of aggression and the arms race in the cyber environment.

One of the problems that are not fully clarified by contemporary international law concerns the responsibility of the states that are developing or they are at the origin of a cyberattack on the organs/authorities/institutions of another state. According to article 8 of the Draft Articles on Responsibility of States for internationally wrongful acts, adopted by the UN International Law Commission (RDI) in 2001 "The State is responsible for the acts of a person or group of persons if the person or group of persons acting on the basis of instructions or under the guidance or the control of the appartanance state."[30] Considering a series of cyberattacks that have been consumed in recent history, even was possible to identify and locate the "entities" that have carried out cyberwar actions, it wasn't succeeded to get the responsibility of the state from the territory that the actions were consumed. According to opinions regularly promoted in the specialized literature on cyberbullying, states that were the origin of cyberwarfare actions have never recognized the direct involvement in cyberwarfare actions against another state, nor the support offered to private entities to carry out this kind of action against public or private entities of the hostile state.

Starting May 2019, the Council established a framework which allows the EU to impose targeted restrictive measures to deter and respond to cyber-attacks which constitute an external threat to the EU or its member states, including cyber-attacks against third States or international organizations where restricted measures are considered necessary to achieve the

[28] Kimberly Hsu and Craig Murray, *China and international law in cyberspace,* US-China Economic and Security Review Commission Staff Report, May 6, 2014, pp.1-3, accessed January 6, 2020, on https://www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf

[29] Comunicatul şefilor de state şi de guvern din statele Alianţei prezenţi la Summitul NATO de la Varşovia (8-9 iulie 2016), accessed February 10, 2020, on https://www.mae.ro/node/36635.

[30] Adrian Năstase şi Bogdan Aurescu, *Drept internaţional public. Sinteze*. Ediţia 8, Editura C.H. Beck, Bucureşti, 2015, p.367.

objectives of the Common Foreign and Security Policy (CFSP)". Thus, the sanctions regime is established for individuals or entities associated with them that are responsible for cyberattacks and provides support for such attacks.

Conclusions

The study of the various doctrines and security strategies developed by the state actors, both in the western world and outside this system of states, leads us to the conclusion that all these documents have incorporated elements about the threats that come from the cyberspace. Also, as cyberspace becomes increasingly militarized, the states are developing their own defensive cyber capabilities for protecting against cyberattacks, but also offensive cyber weapons in order to defeat the opponent in cyber conflict or to multiply the military force into an armed confrontation between the states.

Even though the cyberwarfare race has not been clearly defined in the official documents of the states and international security organizations, we believe that the cyberwar actions that have taken place in the world in recent years were created a current that guided states to invest human, material and financial resources, generating an arms race in the cyberspace in which more and more states are participating. It is assumed that this arms race will continue in the future, given the threats from cyberspace, on the one hand, but also the right to self-defence (UN Charter, art. 51) in cyberspace, on the other.

International regulations of cyberspace, from the perspective of cyber warfare and the arms race, are far from satisfactory. Cyberspace remains a less regulated area of international law, but in the coming period, we believe that the cyber powers (China, US, Russia, etc.) will continue to strive for cyberspace governance to provide greater security to the world's states and provide viable solutions for reducing the effects of cyberwar actions. Since there is currently no international consensus regarding the definition of "cyber weapon", the prospect of a cyber arms control treaty remains a desire of states, international institutions with attributions in the field of security, but also for the specialists of international law. We believe that in the near future, as other treaties on arms control have been adopted, the states will find the way to reach a consensus, based on well-established norms, which will regulate the cyberwar and limit the cyberspace militarization.

BIBLIOGRAPHY

1. Atlantic Council, *International Law and Cyber Operations* - Launch of the Tallinn Manual 2.0, Washington, 8 February 2017.
2. Barbieri, Cristian, Dernis, Jean-Pierre and Polito, Carolina, *Non-proliferation Regime for Cyber Weapons. A tentative study*, Instituto Affari Internazionali (IAI), Documenti IAI18/03-March 2018.
3. Băhnăreanu, Constantin, *Cursa înarmărilor în arcul de insecuritate din vecinătatea estică a Uniunii europene. Consecinţe pentru România*, Editura Universităţii Naţionale de Apărare "Carol I", Bucureşti, 2010.
4. Clapper, James R., Marcel, Lettre and Michael, S. Rogers, *Foreign Cyber Threats to the United States,* Joint Statement for the Record to the Senate Armed Services Committee, 5 January 2017.
5. Corera, Gordon, *Rapid escalation of the cyber-arms race,* BBC News, 29 April 2015.
6. Craig, Anthony and Valeriano, Brandon, *Conceptualising cyber arms races*, 2016 8th International Conference on Cyber Conflict, 2016 © NATO CCD COE Publications, Tallinn, p.142.
7. Dungaciu, Dan (coord), *Enciclopedia relaţiilor internaţionale*, Vol.I, Editura Rao, Bucureşti, 2017.

8. Fábián, Gyula, *Drept internaţional public. Note de curs*, Editura Hamangiu, Bucureşti, 2019.
9. Goldstein, Joshua S. şi Pevehouse, Jon C., *Relaţii Internaţionale,* Editura Polirom, Iaşi, 2008.
10. Herz, John, *Idealist internationalism and the security dilemma,* World Politics, 2 (2). 1950.
11. Hsu, Kimberly and Murray, Craig, *China and international law in cyberspace,* US-China Economic and Security Review Commission Staff Report, May 6, 2014, pp.1-3.
12. Intriligator, Michael D. and Brito, Dagobert L., *Arm races*, Defence and Peace Economics, February 2000, Vol 11 (1).
13. Kissel, Richard (ed.), *“Glossary of Key Information Security Terms”,* in NIST Interagency/Internal Report (NISTIR), No. 7298rev2 (May 2013).
14. Miroiu, Andrei şi Soare, Simona, *Balanţa de putere,* capitol cuprins în volumul Manual de relaţii internaţionale, coord. Andrei Miroiu şi Radu Sebastian Ungureanu, Editura Polirom, Iaşi, 2006.
15. Năstase, Adrian şi Aurescu, Bogdan, *Drept internaţional public*. Sinteze. Ediţia 8, Editura C.H. Beck, Bucureşti, 2015.
16. Norden, Lawrence and Weiner, Daniel I., *US election are still not safe from atack*. Congress can change that it if acts fast, Foreign Affair, July 23, 2019.
17. Robinson, Paul, *Dictionar de securitate internaţională*, Editura CA Publishing, Cluj Napoca, 2010.
18. Schmitt, Michael N. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge, Cambridge University Press, 2017.
19. http://www.bbc.co.uk/ news/uk-32493516
20. https://www.researchgate.net/publication/305871947_Conceptualising_cyber_arm races
21. https://www.ruf.rice.edu/~econ/papers/1999papers/01Brito.pdf
22. http://www.iai.it/sites/default/files/iai1803.pdf
23. https://www.foreignaffairs.com/articles/russia-fsu/2019-07-23/us-elections-are still-not-safeattack?utm_medium=newsletters&utm_source=fatoday&utm_content=20190723&utm_campaign=FA%20Today%20072319%20U.S.%20Election%20Security%2C%20Brexit%20and%20British-EU%20Ties%2C%20Tensions%20in%20the%20Strait%20of%20Hormuz&utm_term=FA%20Today%20-%20112017
24. https://www.nist.gov/node/579721
25. https:// www.armed-services.senate.gov/download/clapper-lettre-rogers_01-05-17.
26. https://www.consilium.europa.eu/ro/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

Information Systems, Intelligence And Cyber Security

Chairs:

Dănuț TURCU, PhD
Ion CĂLIN, PhD

EU CYBERSPACE STRATEGIC DOCUMENTS

Marius PĂUNESCU
"Carol I" National Defence University
paunescu.marius@unap.ro

Abstract: *European citizens' future security depends on transforming their ability to protect against cyber threats. Because both civilian infrastructure and military capacity rely on secure digital systems, cyberspace has generated many challenges to nations in the process of upgrading their understanding, capabilities and actions which preserve freedom and security for individuals in the Information Age. Therefore, a traditional approach of building a national security strategy which gives responses to the threats coming from outside and inside is no longer valid in the cyberspace where physical boundaries do not exist, and the adversary is not all the time clear identified. In the context of the "cyber awakening" at the national and internatinal level, this article presents the EU work on a couple of strategic initiaves, such as Network and Information Security: Proposal for A European Policy Approach, Strategy for a secure information society – Dialogue, partnership and empowerment, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, The European Agenda on Security, Global Strategy for the European Union's Foreign and Security Policy – Shared Vision, Common Action: A Stronger Europe, and the Joint communication to the European Parliament and the Council – Resilience, Deterrence and Defence – Building strong cybersecurity for the EU, in order to control the cyberspace in an open, safe and secure manner and bridge the gap between existing needs, deeds and regulations.*

Keywords: *EU, cyberspace, cyberdefence, strategy, security.*

Introduction

A traditional approach of building a strategy is to identify desired ends, ways and means on three dimensions: external dimension (responses given to the threats coming from outside), internal dimension (responses given to the threats coming from inside), and the transformational dimension (responses through which every new strategy of security and defence must keep alive the ability to adapt itself to the threats that are constantly evolving).

At present, this approach seemed to be insufficiently adapted to the current needs of security, in which a society no longer operates only in spaces such as land, air, maritime, but also in spaces such as cyber and cosmos. Consequently, in order to secure the national vital interests such as security of the home territory, safety of citizens at home and abroad, economic prosperity, and development of the way of life that generate security for the entire society, today it is no longer sufficient to undertake actions and achieve security objectives in the terrestrial, aerial, maritime security domains, but also in cyber and cosmic space.

Therefore, whether on land, air and maritime space, the states manifest their sovereignty from both the perspective of domestic law and that of international law, in terms of cyber and cosmic space, the state shades its sovereignty as a result of reduced control capacity due to the digitalization phenomenon which is expected to continue creating benefits for individuals through the use of emerging technologies like 5G or the Internet of Things, but also could raise certain challenges related to protection of human rights (e.g. personal data protection, privacy, intellectual property), democracy (e.g. election process, e-governance) and rule of law (e.g. cybercrime).

Bearing in mind that strategy is about "how nations use the power available to them to exercise control over people, places, things, and events to achieve objectives in accordance with their national interests and policies"[1], the challenge for the strategic decision-makers is to coordinate the various instruments of power in a synchronized and integrated fashion to achieve safety of citizens at home and abroad using the cyberspace in an open, transparent and safe manner.

For this purpose, on 16th April 2015 governments, intergovernamental organizations and private companies created a pragmatic Global Forum on Cyber Expertise (GFCE) to build cyber capacity and expertise within the framework of existing international law, in particular the United Nations Charter, the Universal Declaration on Human Rights, the International Covenant on Civil and Political Rights and the UN Guiding Principles on Business and Human Rights. In accordance with its foundation document, the Hague Declaration, the GFCE's provides "a dedicated, informal platform for policymakers, practitioners and experts from different countries and regions to facilitate a) Sharing experience, expertise, best practices and assessments on key regional and thematic cyber issues. […]; b) Identifying gaps in global cyber capacity and develop innovative solutions to challenges; c) Contributing to existing efforts and mobilise additional resources and expertise to build global cyber capacity in partnership with and according to the particular needs of interested countries, upon their request."[2]

In the context of the "cyber awakening" at the national and internatinal level, in order to control the cyberspace in an open, safe and secure manner and bridge the gap between existing needs, deeds and regulations, the EU began work on a couple of strategic initiaves such as: Network and Information Security: Proposal for A European Policy Approach (2001); Strategy for a secure information society – Dialogue, partnership and empowerment (2006); Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013); The European Agenda on Security (2015); Global Strategy for the European Union's Foreign and Security Policy – Shared Vision, Common Action: A Stronger Europe (2016); and the Joint communication to the European Parliament and the Council – Resilience, Deterrence and Defence – Building strong cybersecurity for the EU (2017).

1. Network and Information Security: proposal for a European Policy approach

In 2001, the authors of the Communication from the Commision to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions *Network and Information Security: proposal for a European Policy approach* emphasized the fact that communication services are no longer provided by the state companies but on a competitive basis by many private providers. Whilst this trend of networks transfer from state monopoly to private companies continued amongs a variety of developments in the globalized market, the policy of network and information security had to be changed in order to strengthen "the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems"[3]. At that time, the main security threats were: interception of communications with the purpose to copy data or

[1] ***US Joint Force Development, *Strategy*, Joint Doctrine Note 1-18, 25 April 2018, Unclassified, p.V, available at: https://fas.org/irp/doddir/dod/jdn1_18.pdf, accessed: February 15, 2020.

[2] ***Geneva Internet Platform, DigitalWach Observatory, Global Forum on Cyber Expertise, *The Hague Declaration on the GFCE,* 16 April 2015, Unclassified, p. 2, available at: https://dig.watch/sites/default/files/The%20Hague%20Declaration%20on%20Global%20Forum%20on%20Cyber%20Expertise.pdf, accessed: February 16, 2020.

[3] ***Commission of the European Communities, Communication from the Commision to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions *Network and Information Security: Proposal for A European Policy Approach*, Brussels, 6.6.2001, p.9, available at: https://ec.europa.eu/transparency/regdoc/rep/1/2001/EN/1-2001-298-EN-F1-1.Pdf, accessed: February 16, 2020.

modify; unauthorized access into computers and computer networks with the intent to copy, modify or destroy data; network disruption; execution of malicious software that modifies or destroy data; malicious misrepresentation; environmental and unintentional events (e.g. natural disasters, human error, hardware or software failures, poor management).

To cope with these threats, this document proposed the following measures: awareness raising through public information and education campaign; a European Warning and Information System that can rapidly alert and advise the attacked users and improve coordination through their Computer Emergency Response Teams (CERTs); technology support (research and development); support for market oriented standardization and certification; legal framework coordination within EU's state members; security in government use (e-government and e-procurement activities); international cooperation with international organisations and partners on network and information security.[4]

2. The strategy for a Secure Information Society – "Dialogue, partnership and empowerment" (2006)

The strategy for a Secure Information Society represented a new step in revitalising the achievments of the Communication "Network and Information Security: proposal for a European Policy approach" and embraced three domains: specific network and information security measures; the regulatory framework for electronic communications; and fight against cybercrime.

With the scope of the streghtening the security of the Information Society, the EU proposed a dynamic and integrated approach that empowered every stakeholder to foster awareness of security needs and risks in order to promote network and information security (NIS). In this respect, a quite new European agency, the European Network and Information Security Agency (ENISA), was much more involved in the development of a culture of nework and information security for "the benefit of citizens, consumers, enterprises and public sector organizations throughut the European Union"[5].

In accordance with this strategy, the EU's member states were invited to "proactively participate in the proposed benchmarking exercise of national NIS policies; promote, in close cooperation with ENISA, awareness campaigns on the virtues, benefits and rewards of adopting effective security technologies, practices and behaviour; leverage the roll-out of e-government services to communicate and promote good security practices that could then be extended to other sectors; stimulate the development of network and information security programmes as part of higher education curricula"[6] and the private sector stakeholders were encouraged to take initiatives to "develop an appropriate definition of responsibilities for software producers and Internet service providers in relation to the provision of adequate and auditable levels of security […]; promote diversity, openness, interoperability, usability and competition as key drivers for security as well as stimulate the deployment of security-enhancing products, processes and services to prevent and fight ID theft and other privacy intrusive attacks; disseminate good security practices for network operators, service providers and SMEs as baseline levels for security and business continuity; promote training programmes in the business sector […]; work towards affordable security certification schemes for products, processes and services that will address EU-specific needs […]; involve the insurance sector in developing appropriate risk management tools and

[4] *Ibidem,* p.4.

[5] ***Commission of the European Communities, Communication from the Commision to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions *A strategy for a Secure Information Society* – "*Dialogue, partnership and empowerment*", Brussels, 2006, p.4, available at: https://ec.europa.eu/information_society/doc/com2006251.pdf, accessed: February 17, 2020.

[6] *Ibidem,* p.9.

methods to tackle Information and Communication Technologies-related risks and foster a culture of risk management in organisations and business."[7]

3. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013)

The Cybersecurity Strategy of the European Union represents the first comprehensive strategic document that encompasses the main developments of the last two decades on network and information security and cybercrime. The strategy outlines the principles, strategic priorities and actions, roles and responsabilities for the EU in the cybersecurity domain.

The EU's principles for cybersecurity are[8]:

- The EU's core values apply as much in the digital as in the physical world. There is no difference in the application of laws and norms for the human actions disregarding online or offline behaviours. This principle is in accordance the United Nations Group of Governmental Experts (UN GGE), a UN-mandated working group in the field of information security, that concluded in a report in 2015 that "International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible Information and Communication Technologies environment"[9].
- Protecting fundamental rights, freedom of expression, personal data and privacy. At the level of EU, cybersecurity ought to respect fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union. The EU core values are served by network and information security if NIS is developed and use in accordance with the principles of: "respect for human autonomy, prevention of harm, fairness and explicability"[10].
- Access for all. Digital illiteracy limited or no access to the Internet are barriers for those individuals who wish to live in an Information Age. Everyone should be able to access, through internet, the kind of information he/she needs for proper development.
- Democratic and efficient multi-stakeholder governance. In a globalised world, there are many entities that control the digital networks. Govenmental entities, commercial and non-governmental entities must adhere to common protocol and standards in the future for a proper use and development of Internet resources. Gaining trust between the stakeholders is ensured by the seven key requirements: "human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; environmental and societal well-being; and accountability"[11].
- A shared responsibility to ensure security. All relevant actors, whether public authorities, the private sector or individual citizens, need to recognise this shared responsibility, take action to protect themselves and if necessary, ensure a coordinated response to strengthen cybersecurity.

[7] *Ibidem*, p.9.

[8] ***European Commission, Joint Communication to the European Parliament, the Coucil, the European Economic and Social Committee and the Committee of the Regions – *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels, 7.2.2013, pp. 3-4, available at: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf, accessed: February 18, 2020.

[9] ***European Union, The Common Security and Defence Policy of the European Union, *Handbook on Cybersecurity*, Armed Forces Printing Centre, Vienna/Austria, 2019, p.29, available at: https://op.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1, accessed: February 18, 2020.

[10] ***European Commission, *Ethics Guidelines for Trustworthy Artificial Intelligence*, Independent High-Level Expert Group on Artificial Intelligence, Brussels, 8 April 2019, p. 2, available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai, accessed: February 19, 2020.

[11] *Ibidem.*

The EU's strategic priorities are grouped on five domains[12]:

- Achieving cyber resilience. Cyber resilience refers to the ability to protect electronic data and systems from cyberattacks. In the view of EU, cyber resilience could become more operational if: it is establishe common minimum requirements for NIS at national level; it is set up coordinated prevention, detection, mitigation and response mechanisms, enabling information sharing and mutual assistance amongst the national NIS competent authorities; it is improved the mechanism of preparedness and engagement of the private sector.
- Drastically reducing cybercrime using a strong and effective legislation, enhancing operational capabilities to fight against cybercrime and improvind coordination and collaboration between EU's state members on law enforcement, judicial authorities, public and private stakeholders. In support of this priority, the EU recommends to develop a strong and effective legislation in accordance with the Convention on Cybercrime of the Council of Europe which agreed on substantive criminal law such as[13]: Offences against the confidentiality, integrity and availability of computer data and systems; Computer-related offences; Content-related offences; Offences related to infringements of copyright and related rights.
- Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP) by addressing the invitation to the EU's member states and the European Defence Agency to collaborate in the field of cyberdefence capabilities and technologies (including doctrine, leadership, organization, personnel, training, technology, infrastructure, logistics and interoperability), to protect networks within CSDP missions and operations, to promote dialogue between civilian and military actors in the EU, and to ensure dialogue with international partners. In 2014, the Coucil of European Union elaborated the EU Cyber Defence Policy Framework that identified priority areas for CSDP cyber defence and clarifies the roles of the different European actors for "the development of cyber defence capabilities, made available by Member States for the purposes of the CSDP as well as the protection of the European External Action Service (EEAS) communication and information networks relevant to CSDP"[14]. The policy framework received an update[15] in 2018 in accordance with the Global Strategy on the EU Foreign and Security Policy and within the EU Level of Ambition.
- Develop the industrial and technological resources for cybersecurity by promoting a Single Market for cybersecurity products and fostering Research and Development (R&D) investments and innovation.
- Establish a coherent international cyberspace policy for the European Union and promote core EU values. To address global challenges in cyberspace, the EU will seek closer cooperation with other organisations such as the Council of Europe, Organisation for Economic Cooperation and Development (OECD), United Nations, Organization for Security

[12] ***European Commission, Joint Communication to the European Parliament, the Coucil, the European Economic and Social Committee and the Committee of the Regions – *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels, 7.2.2013, pp. 3-4, available at: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf, accessed: February 20, 2020.

[13] *** Council of Europe, *Convention on Cybercrime*, Budapest, 23.XI.2001, available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561, accessed: February 20, 2020.

[14] ***Council of the European Union, EU Cyber Defence Policy Framework, Brussels, 18 November 2014, p.3, available at: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf, accessed: February 20, 2020.

[15] ***Council of the European Union, EU Cyber Defence Policy Framework (2018 update), Brussels, 19 November 2018, available at: https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf, accessed: February 21, 2020.

and Cooperation in Europe (OSCE), NATO, African Union, Association of Southeast Asian Nations (ASEAN) and Organization of American States (OAS).

4. European Agenda on Security (2015)

The European Agenda on Security, aiming “to bring added value to support the Member States in ensuring security”[16], sets goals and identify priorities regarding the EU action on: 1. *Information exchange* through: Schengen Information System (SIS), Prüm framework, Passenger Name Record (PNR), European Criminal Records Information System (ECRIS), Maritime Common Information Sharing Environment (CISE); 2. *Operational cooperation* through: EU Policy Cycle, Joint Investigation Teams (JIT), Joint Customs Operations (JCOs), Financial Intelligence Units (FIUs), Police and Customs Cooperation Centres (PCCCs), European Judicial Network (EJN), European Public Prosecutor’s Office; 3. *Supporting action* (training, funding, research and innovation) through: CEPOL, Internal Security Fund, Research and innovation.

The agenda identifies three fields of intervention: tackling terrorism and preventing radicalization, disrupting organized crime, and fighting cybercrime. The need to fight cyber crime is based on the reason that EU should protect citizens’ fundamental rights and the economy, as well as to the development of a successful Digital Single Market. Actions in this domain would consist of: “implementation fo existing policies on cybersecurity […]; reviewing and possibly extending legislation on combatting fraud and counterfeiting of non-cash means of payments to take account of newer forms of crime and counterfeiting in financial instruments […]; reviewing obstacles to criminal investigations on cybercrime, notably on issues of competent jurisdiction and rules on access to evidence and information; enhancing cyber capacity building action under external assistance instruments.”[17]

5. Global Strategy for the European Union’s Foreign and Security Policy - Shared Vision, Common Action: A Stronger Europe (2016)

The Global Strategy included cybersecurity in the priorities of the EU External Action together with security and defence, counterterrorism, energy security, and strategic communications. The EU vision on cybersecurity is to equip the EU and assist Member States “in protecting themselves against cyber threats while maintaining an open, free and safe cyberspace”[18]. As a consequence, the EU’s member states should acquire “technological capabilities aimed at mitigating threats and the resilience of critical infrastructure, networks and services, and reducing cybercrime”, should foster “innovative information and communication technology (ICT) systems which guarantee the availability and integrity of data, while ensuring security within the European digital space through appropriate policies on the location of data storage and the certification of digital products and services”, and should weave “cyber issues across all policy areas, reinforcing the cyber elements in CSDP missions and operations, and further developing platforms for cooperation”[19].

6. Resilience, Deterrence and Defence – Building strong cybersecurity for the EU (2017)

The document Building strong cybersecurity for the EU represents a wider plan for the EU to enhance its competitiveness in the field of cybersecurity and to galvanise all actors

[16] ***European Commission, *The European Agenda on Security*, Strasbourg, 28.4.2015, p.2, available at: https://www.cepol.europa.eu/sites/default/files/european-agenda-security.pdf, accessed: February 23, 2020.

[17] *Ibidem*, p.20.

[18] ***European Union, *European Union Global Strategy*, June 2016, p.21, available at: https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf, accessed: February 23, 2020.

[19] *Ibidem*, p.22.

to give a relevant attention to it. This document stresses the need to move from reactive to pro-active and cross-policy approach bringing various work streams together to build EU's strategic cybersecurity autonomy, to improve resilience and response by boosting capabilities (technology/skills), ensuring the right structures are in place and EU cybersecurity single market functions well, to stepp up work to detect, trace and hold accountable those responsible for cyber attacks, and to strengthen international cooperation on cybersecurity and developing cyber defence capabilities.

Its worth to mention that building EU resilience to cyber attacks has a new and valuable instrument – the Directive on the Security of Network and Information Systems which represents the first EU-wide cybersecurity law that is designed "to build resilience by improving national cybersecurity capabilities; fostering better cooperation between the Member States; and requiring undertakings in important economic sectors to adopt effective risk management practices and to report serious incidents to the national authorities".[20] The Directive lays down measures to achieving a high common level of security of network and information systems within the EU by: "a. lays down obligations for all Member States to adopt a national strategy on the security of network and information systems; b. creates a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them; c. creates a computer security incident response teams network ('CSIRTs network') in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation; d. establishes security and notification requirements for operators of essential services and for digital service providers; e. lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems"[21].

Conclusion

Cyberspace understanding and preparedness represent two principal pillars for the Security and Defence of the EU and Member States. The cyberspace strategic documents adopted by the EU hence the ability of the Union and Member States to cooperate with the private sector, including industry and civil society, to find digital technology answers to the daily lives and economies of European society.

The Cybersecurity Strategy of the European Union outlines the need to address responses to cyber threats from three directions – network and information security, law enforcement, and defence – and underlines the need of Member States remain responsible for the prevention of and response to cyber incidents while the EU provides incentives and support to develop and maintain more and better cybersecurity capabilities.

BIBLIOGRAPHY

1. Council of Europe, Convention on Cybercrime, Budapest, 2001.
2. Council of the European Union, EU Cyber Defence Policy Framework, Brussels, 2014.
3. Council of the European Union, EU Cyber Defence Policy Framework (2018 update), Brussels, 2018.

[20] ***European Commission, Joint Communication to the European Parliament and the Council *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, Brussels, 13.9.2017, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en, accessed: February 23, 2020.

[21] ***European Union, Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, Official Journal of the European Union, 6 July 2016, Art. 2, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC accessed: February 23, 2020.

4. European Union, Network and Information Security: Proposal for A European Policy Approach, Brussels, 2001.
5. European Union, A strategy for a Secure Information Society – “Dialogue, partnership and empowerment”, Brussels, 2006.
6. European Union, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 2013.
7. European Union, Handbook on Cybersecurity, Armed Forces Printing Centre, Vienna/Austria, 2019.
8. European Commission, Ethics Guidelines for Trustworthy Artificial Intelligence, Independent High-Level Expert Group on Artificial Intelligence, Brussels, 2019.
9. European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 2013.
10. European Commission, The European Agenda on Security, Strasbourg, 2015.
11. European Union, European Union Global Strategy, 2016.
12. European Commission, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Brussels, 2017.
13. European Union, Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, Official Journal of the European Union, 2016.
14. Geneva Internet Platform, DigitalWach Observatory, Global Forum on Cyber Expertise, The Hague Declaration on the GFCE, 2015.
15. US Joint Force Development, Strategy, Joint Doctrine Note 1-18, 2018.

BLOCKCHAIN MILITARY BUSSINES

Dorin IORDACHE
Assistant professor, "Ovidius" University,
dorin.iordache@365.univ-ovidius.ro

Abstract: *Blockchain technology, the technology behind crypto currencies, will produce substantial changes in the global economy. Blockchain is a new information technology that combines elements of cryptography and the distributed information component. This paper focuses on the basic framework of the blockchain model, its development, the challenges of blockchain technology mainly on information security and decentralized systems. Finally, various applications of current blockchain technology related to the military field are discussed.*

Keywords: *Blockchain, cyber security, decentralization, military business.*

Introduction

Blockchain technology is an opportunity to study how to apply it in military systems since notable achievements are known in the civilian field.

Blockchain is a "*distributed data*" system, having "*block*" the basic component, pooling resources through a peer-to-peer connection so that each block is a unique record that is added to the end of the other block, like a *chain*. The name of the technology, respectively *blockchain* is derived from here, which was described by Satoshi Nakamoto (pseudonym), in the article "*Bitcoin: A Peer-to-Peer Electronic Cash System*"[1], originally as a virtual currency system - bitcoin. The technology was then developed and implemented in different fields: economy, education, medical and even military.

Blockchain[2], in short, is a transaction-based system, generating immutable data collections, managed in a decentralized manner, involving encrypted processes, adopted based on consensus-based trust mechanisms, and optionally defined by a Smart Contract[3].

Blockchain technology - overview

Blockchain technology must initially introduce the concept of virtual currency, provide a storage mechanism and be able to add a high level of security. All this being done in a distributed environment [1]. In time, variants of the initial concept were developed, most of them being functional and they developed more broadly the decentralized component, addressing areas that are wider than that of virtual currencies.. The transactions are marked with a time stamp, arranged chronologically and then grouped into unit entities called *blocks*. The blocks in turn are chained in a logical and well-defined sequence. Hence the name of the technology - *blockchain* - *chain of blocks*. The first entry in the next block of the chain will be the cryptographic hash value (signature / abstract) of its predecessor, thus tying the series of blocks into a chain. This cascading encryption link makes it almost impossible to modify a block in the chain without simultaneous updates to all subsequent blocks. Being a decentralized system, the entire user community has an identical replica of the entire blockchain. If differences of a chain are detected in the decentralized network, the difference is resolved on the basis of one of the consensus schemes: proof of: work (POW), stake (POS),

[1] www.bitcoin.org

[2] Blockchain Technology in Online Voting, https://followmyvote.com/online-voting-technology/blockchain-technology/

[3] https://solidity.readthedocs.io/en/v0.4.24/introduction-to-smart-contracts.html

time, activity, burn, capacity or importance. Each of these consensus methods has advantages and disadvantages.

Each block also includes an additional value called *nonce*, which is selected to ensure that the complete block, when its summary is calculated, will produce a value with one and only a certain result, having a defined number of zero bits in front, possibly, as in the example below (3 zeros).

Structure and content of the block 2 / index =1	
Previous Hash	000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf
Timestamp	1578675586255
Data /Info	Hello
Hash	**00096db550fda00312ff4b41d4eb90750d0a63c59512ba21d16032e26cb30f9b**
Nonce	11345

Table 1. Structure and content of one block [4]

The *hash* value of the current block is determined according to the following scheme:

`SHA256(index + prevHash + Timestamp + Data + Nonce).`

In the above example the *hash* summary value is:

`SHA256(1000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf1578675586255Hello11345)=`

`00096db550fda00312ff4b41d4eb90750d0a63c59512ba21d16032e26cb30f9b`[5]

Blockchain classification includes both unrestricted and authorized models. The original model proposed by Nakamoto [1] is a model without restrictions, in which any user can read and write in the chain. The restricted or private blockchain models [6] maintain distributed content, but reading and writing operations are controlled, based on a central policy. *Mining* processes are easier because they are authorized as well, because miners are restricted users as well. This is positive because consensus is easier to obtain, but it can also be negative if any of the trustworthy elements choose to act destructively, because they act from interior of the structure.

In addition to the ones mentioned above, the structure of a block also includes the digital summary, *hash*, of the root of the Merkle tree [7] of the transactions of that block, similar to the representation in figure 1.

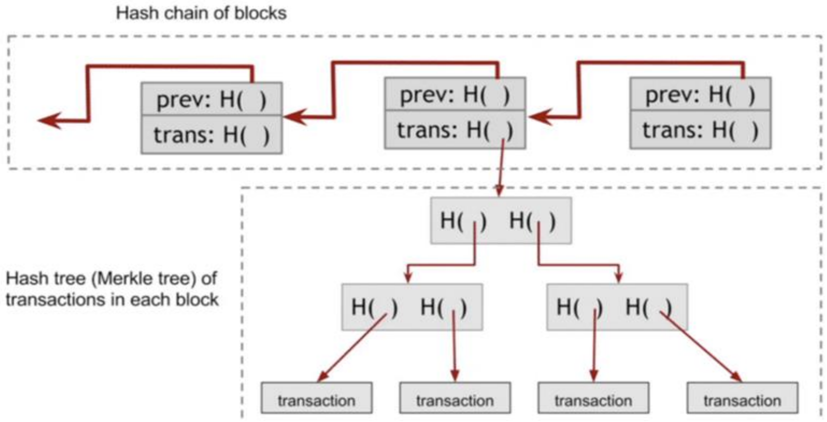


Figure 1. Bitcoin block structure and Merkle tree transaction

[4] https://www.blockchain.com/explorer

[5] Iordache Dorin, Verificarea corectitudinii blocului, https://virtual-academy.ro/Crypto/sha256.html

Merkle binary trees are mainly used in the following fields: data integrity insurance and identical in distributed systems; checking for inconsistency (alteration of data); accurately identifying altered data; virtual coins systems; crypto currencies - storing transactions; version control systems - software and files; certification authorities - maintaining transparent registration of certificates; database management systems - detection of data inconsistency between database copies. From the way the technology and its derivatives from the primary one, bitcoin, have been defined, its area of application is also determined.

Areas of interest of the blockchain

If blockchain technology initially appeared and developed in close connection with virtual currencies, the recent decline in crypto currency quotations could be discouraging in development. But, as new and more practical cases of technology use are developed, the more they develop for different areas of economic, social life, etc.

As with any new technology, there is a significant likelihood of misapplication and over-solicitation in the first few, as recent publications have warned.

Use of blockchain technology in the civil field

Blockchain technology with its distributed component defines systems that provide a trusted service to a group of nodes or parties, who do not fully trust each other, precisely for the purpose of increasing the level of trust.

For this reason, as in any new technology, especially one that has reached these high levels of security, there is a relatively high likelihood of wanting to misappropriate or over-apply the technology[6].

Therefore, more important is the way it is implemented, correlated with the scope of blockchain technology. These aspects are much more important if the military field is concerned.

Thus, we can list some of the areas of applicability of blockchain: distributed systems: InterPlanetaryFileSystem[7], decentralized web services[8] [9] [10], distributed video content[11], distributed virtual social community[12].

If we refer to the area of applicability, we can list some significant examples: governmental, logistics [8], medical [9], educational, etc. Statistically, on each continent there are countries that have adopted and implemented projects based on blockchain technology [10].

Blockchain technology military business

Starting from the basic characteristics of blockchain technology, namely decentralization and the immutable nature of the information stored in the block, the military domain cannot be bypassed and even demands the implementation of this technology, considering the specificity of the military activities: confidentiality, availability of systems and services, including information [11][12].

The vulnerabilities generated by determining the location of a person, in the absence of a GPS signal, represent a current concern of the emergency systems, as well as the scientific environment. One of these systems is based on the locations of Wi-Fi points and / or

[6] https://cachin.com/cc/papers/cons-edcc.pdf

[7] https://ipfs.io/

[8] https://awesome.ipfs.io/apps/

[9] https://storj.io/

[10] https://tardigrade.io/

[11] https://d.tube/

[12] https://steem.com/entrepreneurs/

mobile relays. Therefore, to increase the level of availability of information regarding the position of these points, based on which the location of a point can be determined, in the absence of the GPS signal, we can use blockchain technology, in particular the decentralized component, as in figure 2:

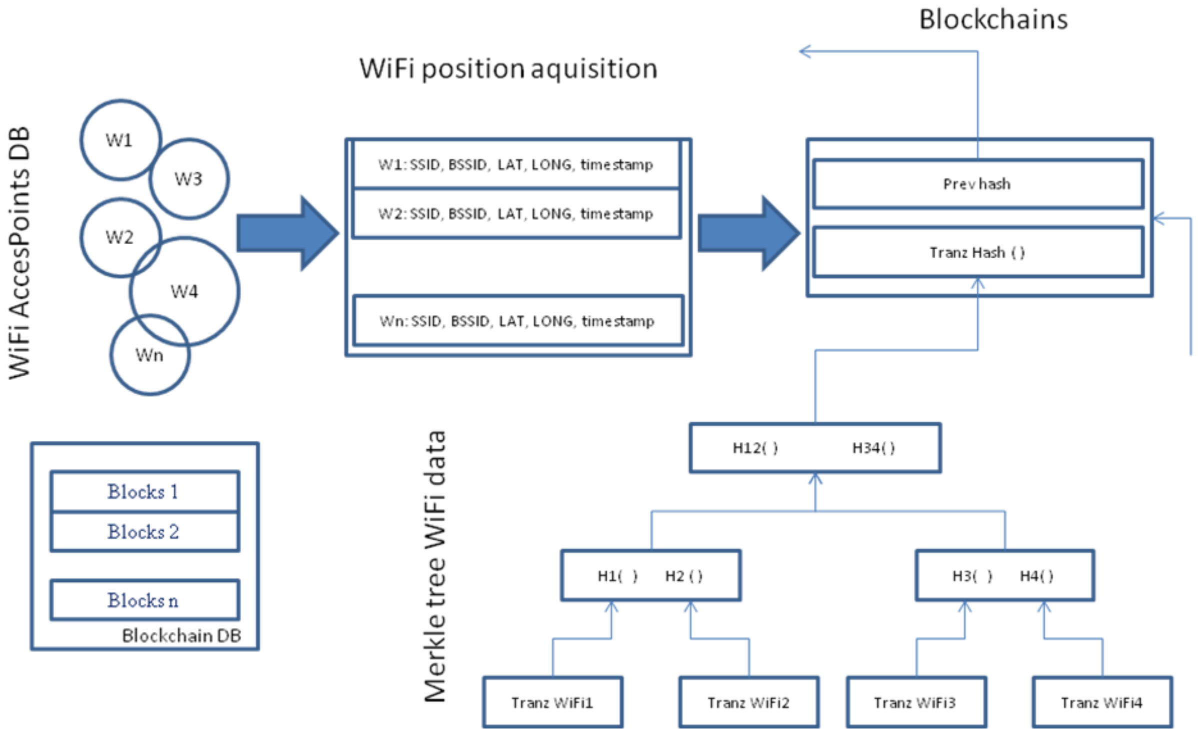


Figure 2. Wi-Fi access point data blockchain architecture

Using a decentralized system for managing each collection with access point data increases substantially, both system security and its availability.

The benefits of blockchain technology are easy to understand when they are represented as distinct use cases, such as major use cases related to defence. [13], respectively: defence of critical weapon systems; managing automated, swarm systems; validation of orders and information on the battlefield; managing logistics and supply chains[13].

The military field can adopt and implement this technology in the field of information with a short duration of updating and resistant in time, as well as the area of distribution systems. This is because a centralized and hierarchical system, which are the basic characteristics of one in the military field, bring disadvantages in what means its discontinuity in certain situations.

We can conclude that blockchain technology represents an opportunity for exploration, but its advantages and disadvantages must be taken into account, including: they use excessive energy; it cannot be a huge distributed computing system; mining does not ensure network security; blockchain entries are not immutable; the life span of a block is not infinite; reduced flexibility; it is not an indestructible technology; the anonymous / open character of blockchains is not necessarily an asset, especially in the military; Proof of Work is excessive, both in terms of time and resources; they can generate complexity instead of simplicity; can be inefficient.

[13] Navy Raises Anchor on Blockchain, https://www.afcea.org/content/navy-raises-anchor-blockchain

BIBLIOGRAPHY

1. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System, October 31, 2008***,** https://bitcoin.org/bitcoin.pdf
2. Don Tapscott, Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, May 10th 2016, Portfolio, ISBN 0670069973
3. Ethereum is a global, open-source platform for decentralized applications, https://ethereum.org/
4. IPFS powers the Distributed Web, https://ipfs.io/
5. Hyperledger – Open Source Blockchain Technologies, https://www.hyperledger.org/
6. Chris Chinchilla, *A Next-Generation Smart Contract and Decentralized Application Platform*, Jun 17, 2019, https://github.com/ethereum/wiki/wiki/White-Paper
7. Ralph Merkle, "*A Certified Digital Signature*" , 1979 https://www.researchgate.net/publication/221355342_A_Certified_Digital_Signatur
8. TradeLens blockchain-enabled digital shipping platform continues expansion with addition of major ocean carriers Hapag-Lloyd and Ocean Network Express, July 2, 2019, https://www.maersk.com/news/articles/2019/07/02/hapag-lloyd-and-ocean-network-express-join-tradelens
9. Express Medichain – A Healthcare Blockchain Revolution, https://steemit.com/cryptocurrency/@mikerowave/medichain-a-healthcare-blockchain-revolution
10. A comprehensive list of public sector blockchain experiments planned, in progress, or paused globally, https://consensys.net/blog/enterprise-blockchain/which-governments-are-using-blockchain-right-now/
11. Salvador Llopis Sanchez , *Blockchain technology in defence*, EDA Project Officer, Cyber Defence Technology, https://www.eda.europa.eu/webzine/issue14/cover-story/blockchain-technology-in-defence
12. Brig. Gen. Mark T. Simerly and Daniel J. Keenaghan, Blockchain for military logistics, October 1, 2019, https://www.army.mil/article/227943/blockchain_for_military_logistics
13. *Dr. Victoria Adams,* Why Military *Blockchain is Critical in the Age of Cyber Warfare,* Consensys Government Practice Lead in Washington D.C**,** https://media.consensys.net/why-military-blockchain-is-critical-in-the-age-of-cyber-warfare-93bea0be7619

FROM MEGATRENDS IN HIGH TECHNOLOGIES TO EVERYDAY CYBER DIPLOMACY'S PRACTICE

Cristina BODONI
PhD student, "Carol I" National Defence University
cristina_bodoni@yahoo.co.uk

Abstract: *After resisting at innovation, diplomacy let the digital tools entered it in the resilient diplomatic practice based on informational tools, hybrid activities. The bold diplomats started to open their virtual embassies and websites for the Ministries of Foreign and International Affairs, in hope to become a successful diplomatic representative. Then, the cyber diplomats tried to find the common paths to legalize the universal chaotic internet. From the trends of the 2010s to have an active account on the net on any famous social media network, national diplomatic systems take a step forward, they implement more advanced types of information tools. In the last two years, the cyber diplomats have unlocked Pandora's box. This Pandora 2.0 box is filled with the high-tech gadgets, internet and 5G systems, the blockchain, the metadata, clouds, artificial intelligence or empowered memory computers, explained in the technology megatrends for the next decade of the 2020's.*

Keywords: *cyber diplomacy, diplomacy, high tech gadgets, security, cybersecurity*.

Preamble

We live in times when the security of having a service is very low, the instability is growing and the way we perceive reality begins to differ from what was a *normal* one for us, where each one had his work rhythm, each group had his own cultural organization, each nation or population had its own values. If everything is reinterpreted, the diplomatic practice has not escaped to this change. We have cyber diplomacy used for every diplomatic activity for facilitating the interconnectivity on cyber space.

In the early age of the 2000's we hardly heard about artificial intelligence outside of science-fiction stories or movies. In some specific activities, as marketing online and technological design, we used to elaborate our projects knowing about some useful algorithmic formula in design programs or to optimize our websites, we heard about Siri, the personal assistants used by I-phone but we generally neglected the opportunity to interact with it. Then, we found that the personal assistant was developed at the big IT transnational companies, it became Alexa for Amazon and Cortana for Microsoft.

However, everything has changed after 2015. In February 2016, the public opinion around the world was astonished by the interviews with Sophia, the first released humanoid robot by Hanson Robotics from Hong Kong[1]. We immediately found out that there are a lot of different types of artificial intelligence, algorithms or deep learning machineries but we did not care as long the producers kept a low profile on the specificity of all high-technology gadget.

From traditional diplomacy functions to cyber diplomacy ones

The United Nations (UN) Chart specifies the fundamental principles of diplomacy agreed on international relation, the UN state members transformed the principles in diplomatic functions after entered in force the Vienna Convention on Diplomatic Relations (1961) and Vienna Convention on Consular Relations (1963). Some of these functions are

[1] Ben Goertzel, Gino Yu, *Loving AI:Humanoid Robots as Agents ofHuman Consciousness Expansion (summary of early research progress),* from September 25, 2017, accessed January 20, 2020, on www.arxiv.org/pdf/1709.07791.pdf, pp. 1-3.

about representativeness, the collecting and structured information, report and communicate, fostering dialogue, harmonize interests, develop cooperation and exchanges among countries[2], built and maintain bi/multilateral relations, principles of representation and mediation, non-interference in domestic affairs.

The historic tradition in diplomacy is about reciprocity, to maintain functional, structured diplomatic relation, that built and maintain public relations with multimedia and the opinion public.

The four trumps of cyber diplomacy are[3]: the representation of the capacity of governments to deploy digital resources in digital environment as is their ability to control them through state intervention in access to the Internet and social media, the second one is related to changing foreign policy agendas, the other facet of the cyber diplomacy environment focuses on cyber agendas, as operated malicious program into a computer, or Russian "interference" in the US presidential elections have only served to enhance growing concerns with cybersecurity. The third focuses on the use of the Internet and related digital technologies for knowledge management. This not only strengthened the arguments of those questioning the relationship between headquarters and diplomatic posts as MFA network, it is about changing MFA procedures within the organization as a whole. The last one, is about digital technologies to enhance the performance of the public service, reinforce participation in policy shaping.

The all kind of information programs, as deep learning, algorithms, chatbots or AI, are made to facilitate the humankind' life, to prevent or face the challenges and threats, in accordance with all hierarchical jobs from the lowest functions of administrative one to the highest political and diplomatic level.

From the 2018' megatrends in the field of high technologies to the diplomatic and consular practice in 2020's

In the next years 2020 - 2030, the central ideas will emphasize each trend, it will grow exponentially because of desire to have a profitable business, to gain more money with less effort and allocated time for working, the resistance at unpredictability and change; technology is facilitating sharing, collaboration and changes; develop smart cities and businesses, care for the environment; the diversity of the digital working environment, with additional facilities and assurances for the health and well-being of the employees, will lead to changes in the classical organization of the institutions responsible for the implementation of the foreign policy, especially for cyber diplomacy. In contrast with all these advantages, the interconnectivity through high-tech gadgets could easily destroy the relations, empathy, we have already seen in the forming of particular hubs and group polarization. Thus, opening to the outside world through the Internet has become an extension of man. This area is built from nodes and interconnected networks without borders and must be secured.

With all these aspects explained, could be cyber diplomacy take the baton from the traditional one?

Samantha Bradshaw does not trust Cyber diplomacy, she is a skeptic digital diplomat, concerned about the exposed diplomacy on social media. "…*While the Internet has revolutionized our world over the past 10 years, we should not throw away old methods of engagement. Accessing information online is not the same as having on the ground, first-hand experience. Having a conversation with stakeholders behind a computer screen is not the*

[2] *** *Ratificarea Conventiei de la Viena cu privire la relatiile diplomatice*, încheiat la Viena la 18 aprilie 1961, accessed 15, 2020 on ww,w.mae.ro/sites/default/files/file/acte_normative/2006.03.29_viena_1961.pdf

[3] Brian Hocking, *Communication and Diplomacy: Changeand Continuity*, pp. 79 -97, in vol. Thierry Balzacq, · Frédéric Charillon, Frédéric Ramel (Editors), *Global Diplomacy. An Introduction to Theory and Practice,* Editura Palgrave MacMillan, SpringerNature, Cham, Switzerland AG 2020, pp. 83 – 88.

same as talking face to face. Substituting online forums for embassies would be a mistake…[4]," but we think positive about it thanks to other schools of diplomacy, where big steps are made in international and cyber diplomatic environment. The number of cyber diplomats is still small, but nation states are realizing the importance of this new type of diplomacy. Countries like Germany, Finland, USA, Canada and Australia have similar posts as Estonia's Ambassador at Large for Cybersecurity, Tiirma Klaar[5]. France founded the first specific function for cyber space, one of the Secretary of State from Ministry of Foreign Affairs is responsible for cyberspace problems. Denmark opened the first tech-embassy in Silicon Valley, in 2017. In European Union (EU), from 2017, the GDPR, a European Directive (specific EU rule of law) for cyber space is in force.

Therefore, these changes indicate that megatrends in high-tech surpassed the idealist people who dreamed to have internet everywhere and anytime, at work and at home, included in all three power of state, in legislative, executive and jurisdiction. We adapted these to Cyber diplomacy, as follows[6]:

- The cyber diplomacy is the cyber unarmed arm of the state beyond its borders. Through cyber diplomacy the national governments could engage in real-time in international and jurisdictional forums to address interconnected issues using meta-data/clouds assisted by data analytics and some artificial intelligence as Sophia (The cheapest version of a little educational robot cost starts from 5$).[7]
- Another function of diplomacy is to negotiate and sign international treaties. Through Cyber diplomacy, it could immediately detect the inadvertence during the negotiation, the mistake and so on.
- Through Cyber diplomacy the state could encourage behavioral change among diaspora to manage the impacts where the proposed changes have been ineffective, example, the voting through correspondence; to make lobbies for national investors in the domestic markets from the host country; to find the best practices, policy priorities and choices for foreign investment in sending state;
- Involvement in public policies, where it is necessary more holistic long-term view on infrastructure of information systems.

At the end of 2018, there Marr presumed nine trends in high technologies[8]: Metadata would become datafication of every lives; the popularization of The Internet of Things (IoT); the exponential growth in computing power; The incredible rise of artificial intelligence (AI) and computers; The unstoppable freight train that is automation; 3D printing opens up amazing opportunities for manufacturers, We're interacting with technology in very different ways, as with Siri, the personal assistant from I-phone; blockchains; and the platforms for different activities and professions would enter in the routine of professionals.

The former trends for high technologies and the digital sphere from the end of 2018, at the beginning of the year, 2020, most of them are in an advanced stage of implementation in private and public organizations.

[4] Samantha Bradshaw, *Digital diplomacy - #notdiplomacy,* Canadian Government Executive, Aprilie 7, 2015 accessed January 10, 2020, on www.cigionline.org/articles/digital-diplomacy-notdiplomacy.

[5] Már Másson Maack, *What the hell is a 'cyber diplomat'?* July 2019, accessed January 10, 2020, on thenextweb.com/eu/2019/05/24/what-the-hell-is-a-cyber-diplomat/

[6] *** Mowat Centre. *Future State 2030: The global megatrends shaping governments assets,* accessed January 10, 2020, on www.kpmg/content/dam/kpmg/pdf/2014/02/future-state-2030-v3.pdf, pp. 5, 52 – 57.

[7] *** *Newest early education toys Google assistant artificial intelligent AI voice early educational companion robot for children,* accessed January 10, 2020, on www.alibaba.com/product-detail/Newest-early-education-toys-Google-assistant_60786539950.html?spm=a2700.galleryofferlist.0.0.67015c27IqfyvV

[8] Bernard Marr, *9 Mega Technology Trends And How They Are Re-Shaping Our World,* accessed January 10, 2020, on www.bernardmarr.com/ebooks/9-Mega-Technology-Trends-eBook, 2019, pdf, pp. 6, 17, 29, 41, 54, 65, 75, 89, 100.

From all nine high-tech megatrends, cyber diplomacy uses many of the above listed, as data, clouds, sharing information, If we discuss about chat, dialog, document exchanging through different social media portals, websites messages, e-mail, everybody leaves personal information, its mark, a name, a document, an email address or a telephone number. The sum of all these are data, with each time we pass by we increase *datafication* in institutional servers or in clouds.

The internet of things is not so much used in diplomacy, but the institution includes open-minded and smart people. And if they use it in privacy, the institution is in danger, especially without a proper cyber security program for protecting information tools because internet of things is about sharing information in real-time, where deep learning, algorithms and artificial intelligence is changing and learning one from other.

Entering in the spiral of cyber-innovation, robots, gadgets to empowering the memory of each augmented and virtual reality, artificial intelligence, or quantum computer provoked a real tremble for each of us. From being happy to use all these tools, the simple users started to feel the new high technologies as the closest menaces for their jobs and lives, and the diplomacy make no exception, because as in traditional practice, in cyber diplomacy we need some specific qualities, there the main strengths are about how to engage in constructive dialogue, for negotiating and mediating, but the dialogue cannot take place if one of the participants does not pay attention to another one; then, in dialogue you need empathy in order to understand from the perspective of the interlocutor; assertiveness, ability to initiate a conversation, to make sincere compliments, without hidden interests, the ability to always constructively criticize and receive justified criticism and kindness. Exactly as the transformation of artificial intelligence (AI) in being kind and patient. The new programs of this AI are to replace the employees in services where hard work, danger, patience and empathy are extremely needed. Therefore, an AI can be a good trainer for a diplomat before going to mission, it can replace one on the phone when it is necessary to provide information and facilitate the exchange of documents etc.

Also, by means of algorithms, false and fake identities or dangerous people can be detected in time, which can lead to the prevention of difficult situations and the preparation to face the challenges and threats, in accordance with the commitments at the highest political level.

It should not be forgotten that from the antic philosophe Protagoras affirmation: *people remain the measure of all things*, nothing has not changed yet. People think on innovations, constructs the programs, as well they can destroy them or to spoil them just like in the past, when the electric machinery provoked the same feeling. However, the information system has an important component made up of algorithms, bots or robots.

If the people remain the measure of all things, why not use all kind of innovation to avoid *the four Ds. " Dull, dirty, dangerous and dear jobs, where the machinery work faster, safer, cheaper and more accurately"*[9].

In cyber-diplomacy, using blockchain technology is a practical solution to different situations linked with the vote abroad, issuing documents for the citizens abroad, either in transit or Diaspora. The connections with the other states can be made easier in the case of visa applications, for data verification, the situation regarding the legal record of those interested in the visa.

The blockchain is a concept taken from the verification structures of cryptocurrencies. This is a web of blocks made of different stored, ensured, checked, monitored, and protected metadata. The verification anchors for security are proportional to the number of nodes in the

[9] Bernard Marr, *9 Mega Technology Trends And How They Are Re-Shaping Our World,* accessed January 10, 2020, on www.bernardmarr.com/ebooks/9-Mega-Technology-Trends-eBook, 2019, pdf, pp. 54-65.

network, the node represents a block in the blockchain. There the data security technology is easier to maintain; the single point of failure is the user.

At the international level, a blockchain system can be a government information system, and blockchain systems are like state systems related to the digital platforms currently used. Another implication for this blockchain in diplomacy is a more efficient use in the field of economic diplomacy, to mediate business and investment for the sending state. Using blockchain as a platform, the economic diplomacy extends its role of the facilitator for making business interactions online.

Post amble

In cyber diplomacy we noticed a plethora of tendencies, some extremely necessary for adjusting the conservative system of diplomats, others totally unnatural for the diplomatic world.

The probabilities for the development of technologies based on artificial intelligence, algorithms and deep learning had been designed to put into circulation in the following 10-15 years, but they silently entered much earlier in our lives, much faster than the scientists anticipated. The alleged trends for the next decades were outdated.

In 2020's, we live in the times when *Nihil simul inventum est et perfectum* have never been more real, the invention and the popularity of all achieved technological tools are perfectible. As soon as you buy a new high-tech gadget, you discover that something else is better. The way in which we interfere with the new technologies on new paths that go beyond the places of the physical spaces induces the idea that we form a genuine trichotomy, where neither the clouds nor the sky will ever be the limit, as long as clouds mean a virtual place for stocking information, virtual helmet and other augmented reality gadgets or virtual reality tools become a *second life*. For the real life, in the very close future, gathering tools from this Pandora 2.0 box people will pass over it in search of adventure or a new home, both ways, real and virtual through.

These are the times when cyber diplomacy has come into the complicated domain of diplomacy with its innovated activities that required different capabilities such as: the power to easily adapt to change and mobility, collaboration and participation, sharing information or/and keeping them safe online.

BIBLIOGRAPHY

1. *** *Ratificarea Conventiei de la Viena cu privire la relatiile diplomatice*, încheiat la Viena la 18 aprilie 1961,
2. Balzacq, Thierry; Charillon, Frédéric, Ramel, Frédéric, (Editors), *Global Diplomacy. An Introduction to Theory and Practice,* Editura Palgrave MacMillan, SpringerNature, Cham, Switzerland AG, 2020
3. www.mae.ro
4. www.arxiv.org
5. www.cigionline.org
6. www.thenextweb.com
7. www.kpmg/content/dam
8. www.alibaba.com
9. www.bernardmarr.com

THE ENDEAVORS OF CYBER DIPLOMACY TO PROMOTE THE NATIONAL SECURITY IN THE SECOND ERA OF INTERNET

Cristina BODONI
PhD student, National Defence University "CAROL I",
cristina_bodoni@yahoo.co.uk

Abstract: *The bug words of today's information world are technology and digitalization, cyberspace and cybersecurity. The inventions of every tools and activities in cyberspace brought to our life the constant and rapidly change which influences the behavior of state and non-state international actors, leaving them no time to get used to each stage separately. The rapid immersion in the informational age of humanity provoked shock after shock, causing immunity symbolically called resilience. Nowadays everything is smart, resilient, technological in analog or digital networks. All these have produced effects on the behavior of public institutions, causing them to adapt to the unprecedented challenges in extremely conservative fields such as diplomacy, transforming it into cyber diplomacy (with its synonyms, e-diplomacy, digital diplomacy, real-time diplomacy, etc.). By a closer glance, we observe that the cyber diplomacy is far more than a simple tool for using the online platforms for press communication or to inform the public opinion on some events or to promote diplomatic activities.*

Keywords: *cyber diplomacy, diplomacy, high tech gadgets, security, cybersecurity*.

The conundrum.
The tricky puzzle of entailing cyber diplomacy in sensitive domain of security, from the cause to the endeavor

> *"In more conventional arms control or non-proliferation talks, diplomats only talk to diplomats and they don't really need input from other communities.*
> *But in the field of cybersecurity, you need to talk to all stakeholders because you need to keep up to date on all technological development[1]."*
>
> *Tiirmaa-Klaar*

Over the years of academic research on national security and cyber diplomacy niches, we have noticed that the extension of diplomacy in the information environment is directly related to the level of trust in national security infrastructures and diplomats' confidence in their national security and national geostationary or satellite communication systems.

Moving on to the Cold War, the monopoly of geostationary satellites was held until the 1980s by the two Great Powers of the Cold War, Russia (the nowadays legitimate heir of the USSR) and the United States of America, the Soviet GLObal NAvigation Satellite System (GLONASS) and the American Global Positioning System (GPS). In the 80's, India and France ended that monopoly with the French Ariane and the Indian Apple satellite communications systems[2]. During the 2000's, China launched the BeiDou (BDS or

[1] Már Másson Maack, What the hell is a 'cyber diplomat'? from July 2019, accessed January 10, 2020, on thenextweb.com/eu/2019/05/24/what-the-hell-is-a-cyber-diplomat/

[2] R.M. Vasagam, *APPLE in Retrospect, Indian First Communication Satellite – APPLE*, pp. 264-274, in vol. P.V. Manoranjan Rao (chief editor), *From Fishing Hamlet to Red Planet*, Harper Collins Publications, New Delhi, India, 2016, pp. 264-265.

COMPASS)[3] followed by Japanese Quasi-Zenith Satellite-1 Michibiki[4]. The member states of the European Union decided to have their own satellite navigation system, Galileo, launched in 2011[5].

This complex observation has been the result of finding answers to the five W's questions and two H's ones regarding the pioneer states that implemented cyber diplomacy; the causes were transformed into opportunities by those diplomacies and there was a possible relationship between the estimated national security system, ICT and diplomacy systems.

We found at the forefront of cyber diplomacy those countries that had implemented at a satisfactory level the adequate national and outer-space infrastructures to adapt the diplomacy in cyber space. Also, in this situation we found the states that were members of NATO and European Union, implicitly and explicitly. They were strategic partners with the United States. We consider as pioneers of cyber diplomacy the USA, Japan, the People's Republic of China, the Russian Federation. Then, after the US' cyber diplomats, the Mexicans and Canadians diplomats entered in cyber diplomacy, as well as some member States of the European Union diplomats from United Kingdom of Great Britain and Northern Ireland, Sweden or Italy who had the audacity to develop the diplomatic practices in the virtual space.

Defining cyber diplomacy and its main objectives in the second era of internet

The cyber diplomacy came into the diplomatic practice by connecting two generic used words in nowadays life, cyber and diplomacy. The cyber space is the place where diplomacy extended its practice through information and communication~~s~~ technologies (ICTs) in the second era of the internet.

Thus, why do we use the second era of internet? And what about the three main powers in the state? After the check-and-balance – legislative, executive and jurisdictional powers –, we use to count the fourth power in state, the media. During the 2010's decade, we started to talk about the four generations of internet and about the industry 4.0., in the conditions where we hardly agreed on the fifth wave of globalization. After that, it came into our attention 5G, the fifth generation of the wireless technology for digital cellular networks. Thus, we will stop at the six generations of people living on Terra at the same time, for the first time in our world history.

Therefore, we remark the human temptation to counter the domains in ages and generations, where we find the same trend to counter diplomacy. We found out that diplomacy is countered from traditional diplomacy as diplomacy 1.0 to diplomacy 4.0., we expect that in the next years this will be used in parallel with other synonyms of digital, cyber or e-diplomacy, the imported name of 5G, as 5G diplomacy, or the following Diplomacy 5.0.
We think that it is time to plug cyber diplomacy in the second era of the Internet. The first age of internet came in humankind life in October 1969. The navigation was without any single rule, everything was possible. The time changed gradually. Thus, the second age of internet has come. In 2020, we use the algorithms, botchats, deep learning and artificial intelligence in diplomatic practice corresponding to its traditional groups of activities: symbolic, political, and legal.

If the first age of the Internet was chaotic, the second one has become anarchic, being similar with the states in the dawn of age of national states after entering into force the Westphalia treaties.

[3] Claudiu Tănăselia, *Sisteme de navigatie prin satelit*, from December 16, 2016, on www.stiintasitehnica.com/sisteme-de-navigatie-prin-satelit/

[4] Takao DOi, *About Quasi-Zenith Satellite-1 "MICHIBIKI*", from September 11, 2010, accessed at January 10, 2020, on www.global.jaxa.jp/projects/sat/qzss/

[5] Claudiu Tănăselia¸ *Op. cit.*

In the first era of the internet, the navigation on the search browsing motors was: chaotic, based on keywords, without borders, the state was almost non-existent, real-world documents were not digitized, property - almost non-existent, only addresses and domains were on the search engines.

The second age of the Internet is anarchic, based on the Westphalian rule valid for states, with national borders and rules, we can find almost all the main elements of the state transposed on the Internet, even the formation of clusters (international organization) of state actors and regionalization of the cyber space[6] are available on the internet.

Thus, cyber diplomacy represents the ability of diplomacy to include digital competences in its day by day practice and the ability to use digital and analog information and communication technologies (ICTs) on diplomatic processes of consular, diplomatic and administrative corps' activities.

The main objective of diplomatic practice in information era should be reduced almost to zero complaints and agility in service. As part of the cyber diplomacy' strategy, the field of cyber diplomacy could include algorithms, robotic inventions and the high technologies gadget added by the following *"four cornerstones: (a) digital journeys include omni-channel journeys, self-service, live contact; (b) process digitization covers the digital and the artificial intelligence workflows, digitization and automation of transactional activities, remote and no touch installation; (c) predictive services take into considerations the maintenance, advanced analytics, care and sales; (d) digital assistants as the digital service bots and artificial intelligence capabilities support agents"*[7].

These cornerstones help us to adapt the in the cyber diplomacy practice in order to achieve its main endeavors: (a) cyber or digital diplomacy include omni-channel international relations with state and non-state international actors as an alternative for the obsolete traditional diplomacy, live contact with all these national and international stakeholders; (b) process digitization covers the digital and the artificial intelligence workflows, digitization and automation of transactional activities in the consular, diplomatic and administrative activities of the foreign services; (c) predictive services take into consideration the maintenance, advanced analytics, care and safety of state interest; (d) digital assistants as the digital service bots and artificial intelligence capabilities support the diplomatic services in scope to protect and promote the national interest outside the national borders of the state.

Being brought together under the umbrella of informational instruments, all these elements lead us to another definition of cyber diplomacy, namely: cyber diplomacy is more than social media and/or an e-mail. The cyber diplomacy is an *extension of diplomatic practice* for each space where it is needed to be practiced, in each subdomain of diplomacy, track one and track two diplomacy, bilateral or multilateral diplomacy, as well as in public affairs, domestic and foreign policies.

The national security and cyber security in the second era of internet

National security represents an ensemble of obligations to maintain a decent level of peace, reliability and confidence for all the inhabitants of the state; including the ability of the state to defend their lives and possessions within its borders; to protect their national interests in international relations. In current trends in the international system of security, national security extends its responsibilities to protect its citizens wherever they live.

In the context of the current multilateral security framework, an important role in ensuring international and regional peace, as well as security, rests with the collaborative

[6] Bernard Ancori, *The Carousel of Time: Theory of Knowledge and Acceleration of Time,* Wiley & Son Publications, London, UK, 2019, pp. 114 – 132.

[7] Nils Urbach, Maximilian Röglinger, *Digitalization Cases. How Organizations Rethink Their Business for the Digital Age*, Springer International Publishing AG, Cham Suisse, 2019, p. 20.

actions between all state and non-state actor structures, as well as active cooperation with other centers of global power, with states and organizations that have a significant share in security of different regions of the world[8]. Almost as a syllogism, if the national security is extended to all spaces, then, it is about promoting and protecting national security in international security from earth to outer space, knowing that the cyber space is an artificial space without physical borders, cyber space, thus the national security could be extend wherever the national interests are required, especially through the cyber space.

In cyber space, everybody who navigates on internet or has an intelligent mobile device (smart phone or I-phone) connected to telecommunication systems through geostationary satellites is exposed to cyber threats related to all types of cyberattacks.

In these conditions, the cyber security is a new developed domain, who’s its industrious methods are to prevent possible intrusions. In time, the IT security has become a self-governing area, profitable with resources worthy of consideration by government institutions, especially for reducing the level of uncertainty and vulnerabilities in cyber space; to better secure the stocked personal data, access to internet and outlook. The automation, the bots, algorithms and other implemented processes in cyber security: reduced the risks, costs and allocated time to detect the malfunctions and repair the damages; it has significantly increased the simple user’s confidence in online services and businesses.

Casey Crane believes that in the coming years the threats listed above will add to the following issues[9]: “*the phishing*[10] *landscape is changing, though email still ranks as the biggest of those threats; increasing use of mobile as an attack vector and targeting of local governments and enterprises via ransomware*[11] *attacks”*.

We observe that the Westphalian state has extended its influence and power also in cyber space, laws, censorship and surveillance mode function as well as in the physical spaces within the borders of the states. For example: from 2010 to the present day, we have been impressed by the influence of social media on the states, starting with the Arab Spring. For days, autocratic governments in the Middle East and North Africa have restricted their citizens' internet access to all sites or social media such as Facebook or Twitter. The demonstrations were violent, autocratic governments changed with others, but democracy did not occur. Nor is Russia an exception. Since 2012, Vladimir Putin has repetitively ventured actions to gain the technical control over the internet. In collaboration with Chinese Government, the Russian Government from Kremlin began to enforce restrictions and be able to cut Russia off from the global internet, saying that the first concern of the government is national security, technology comes after. This was the excuse for blocking more than 4 million websites[12]. From 2018, the communist government from Pekin started to monitor the behavior of its population through a smart social ranking system, build in public-private partnerships. South Africa, Tanzania, and Ethiopia governs decided to imitate the Chinese,

[8] *** Romania. Administratia Prezidentiala. *Strategia Naţională de Apărare a Ţării pentru Perioada 2015 - 2019, O Românie puternică în Europa şi în lume*, Bucuresti, 2015, pdf. p. 5.

[9] Casey Crane, *A look at the emerging trends in cybersecurity this year and a sneak peak at what to expect in the coming year. The Top Cyber Security Trends in 2019 (and What to Expect in 2020),* accessed January 10, 2020, on https://www.thesslstore.com/blog/the-top-cyber-security-trends-in-2019-and-what-to-expect-in-2020/

[10] **Note***: Phishing attack is when attackers send malicious emails designed to trick people into falling for a scam; a cyberattack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is sent from some (public) institutions, organizations, a friend etc.

[11] **Note****: Ransomware is a type of malware from crypto-virology that threatens to publish the victim's data. The majority of ransomware attacks start life as a social engineering exercise, usually in the form of an attachment or malicious link. Also, the malware attacks are typically carried out using a Trojan that is disguised as a legitimate file that the user is tricked into downloading.

[12] Andrei Soldatov, *Security First, Technology Second: Putin Tightens his Grip on Russia’s Internet –with China’s Help,* accessed January 10, 2020, www.dgap.org/system/files/article_pdfs/2019-03-dgapkompakt.pdf., pp. 1-5.

this *smart social ranking system* trend, and no longer confine to the national boundaries of one country[13].

The main endeavor of practicing the cyber diplomacy in scope of promoting the national interests is to maximize the countries' trumps, the power and influence of their state, to increase the level of security of their nation by any means, implicitly and explicitly in all spaces known to humanity.

The long road of humankind digital journey from science fiction to real practice in every known space has just started!

The main digitized activities of the diplomatic practice are already included in the foreign policy strategies. Among the most active sectors of diplomacy, on the agenda of diplomacy in the 2020's we find that the public diplomacy has become public diplomacy 2.0, the classical practices of bilateral and multilateral diplomacy are already adapted to the cyber environment. The challenges in nowadays organizations are related to change, adaptation, efficiency and effectiveness which have transformed the tradition in innovation. The cyber diplomacy should include the virtual tools in a specific strategy where the use of digital assistants would optimize the online activities of the official virtual embassies, this could make a difference in the real world.

The following period the public policies will include some foreign policy agenda because of its no-frontier activities in internet ruled by the cyberspace. In this kind of situation, the foreign policy will include all types of cyber diplomacy's activities carried out on the Internet. From the main traditional diplomatic activities rebooted on the digital one, to the main academic works on cyber diplomacy found necessary to include in diplomacy the following practices[14]: The public diplomacy 2.0; Bilateral and multilateral engagement; building the leverage of controlling and monitoring the inside and outside diplomatic activities; Formal and informal groups built of multilateral experts within the lower level of treaty organizations; Assimilation of stakeholders from different regions and sections; Paying more attention to the natural resources of the online and offline international society.

The good practice of cyber diplomacy will make a difference in the real world, when face to face time will become optimized, people won't waste any more time repeating information, filling in documents and so on. Example, by using keywords or following specific people on social media, we could monitor and control the information regarding the national interests, new policies could be identified, or possible dissatisfaction could be prevented from turning into manifest conflicts.

Therefore, in the information age, nothing has changed for diplomacy. They must continue the same practice, they represent their country, they communicate with people, they promote the national interests of their state in the host state etc. However, the cyber diplomacy is limited by the people's digital competences, their access to internet and by how the diplomat master's digital instruments/high-tech gadgets.

If the diplomatic digital tools can help protect our national security, we must put them to work for their (cyber) nation, from the clouds (in technological terms) as well as on earth (offline), with a predilection on the Internet, where more than half of the world's population is active, at least with what they are accustomed, written and negotiate with all entities on social media.

[13] Stefania Grottola, *Artificial Intelligence and diplomacy: A new tool for diplomacy?*, 10/Dec/2018, accessed January 10, 2020, on www.diplomacy.edu/blog/artificial-intelligence-and-diplomacy-new-tool-diplomats

[14] Corneliu Bjola, *Diplomacy in the Age of Artificial Intelligence*, 11/Oct/2019, accessed January 10, 2020, on www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/ari98-2019-bjola-diplomacy-in-the-age-of-artificial-intelligence

The nowadays diplomats need more independency than in the past to answer directly online, where the delay of the 30 legal days for a decision could provoke a diplomatic situation, especially in the Trump Administration. From 2015, we observed that the diplomatic online campaigns started to be more than a dialogue between presidents of state, the public declarations of presidents of states have strong political implications, allowing its conational and other net citizens to participate at dialogues, in accordance with diplomatic values and principles. The cyber diplomacy will use a clear road map of elaborated transformation process to facilitate the electoral process for Diaspora helped by some botchats, algorithms and artificial intelligence built in common with domestic public institutions with explicit details regarding the personal data for their citizen in the foreign state. All these is not in science fiction, it is happening in all countries from around the worlds.

BIBLIOGRAPHY

1. *** Romania, Administratia Prezidentiala. *Strategia Naţională de Apărare a Ţării pentru Perioada 2015 - 2019, O Românie puternică în Europa şi în lume,* Bucuresti, 2015, pdf.
2. Ancori, Bernard, *The Carousel of Time: Theory of Knowledge and Acceleration of Time,* Wiley & Son Publications, London, UK, 2019
3. Urbach, Nils, Röglinger, Maximilian, *Digitalization Cases. How Organizations Rethink Their Business for the Digital Age,* Springer International Publishing AG, Cham Suisse, 2019
4. Vasagam, R. M, *APPLE in Retrospect, Indian First Communication Satellite – APPLE*, pp. 264-274, in vol. P.V. Manoranjan Rao (chief editor), *From Fishing Hamlet to Red Planet*, Harper Collins Publications, New Delhi, India, 2016
5. https://www.thesslstore.com
6. www.dgap.org
7. www.diplomacy.edu
8. https://thenextweb.com
9. www.realinstitutoelcano.org
10. www.stiintasitehnica.com
11. www.global.jaxa.jp

OFFLINE IN-CITY POSITIONING APPLICATION

Dorin IORDACHE
Assistant professor, "Ovidius" University,
dorin.iordache@365.univ-ovidius.ro

Abstract: *The most popular Global Positioning System (GPS) provides information about location and time in all weather conditions, anywhere, or almost anywhere on Earth, if there is a communication line to four or more GPS satellites. Most of the navigation systems used are based on global satellite navigation (GNSS) systems or inertial navigation system (INS), in order to have a high level of accuracy. The current GPS/INS systems cannot meet entirely the future requirements of certain systems, both civilian and military, for several reasons, such as: GPS signals are weak and unusable in some situation, they are sensitive for jamming and interference, and civil GPS signal is unprotected and is available to the general public. Therefore, it is important to have alternatives to the GPS/INS system, if possible completely independent of it. Nowadays, with the increase of the number of Internet users, the number of WiFi access points have increased. Many of these access points are fixed and can be positioned as positioning points in the absence of the GPS signal. We will investigate how, with what effects and limitations can replace the GPS system these WiFi access points.*

Keywords: *GPS alternatives, spoofing and jamming, WiFi access point.*

Introduction

The issue of positioning in space and time in recent years has become particularly important. This is because many of the elements of daily life depend on the global positioning system GNS, known in the common GPS language. Its importance lies also in the impact on a social component of today's life. Almost every person, user of mobile telephony and smart applications, in the modern world, interacts quite frequently with the positioning system: from games applications, to car navigation applications, tourist, and industrial ones, why not. The large number of such users represents an argument that comes to prove its importance. Only in 2019, over 365 million mobile terminals were sold in the world, according to the Gartner Global smart phones sales study[1], most of them with positioning capabilities and uses.

The elements of vulnerability for these users appear in the absence of the GPS position or its alteration, accidentally or intentionally. If in the case of the users in personal scope the lack or the alteration of the position does not always have negative effects. In contrast, economic operators can suffer considerable financial damage, and in some cases there can be human losses. In the event of an emergency situation and GPS information or Internet connection are not available, the existence of an alternative solution is required.

GPS world Overview

The availability and stability of the GPS signal is a permanent concern of the major global players in the field. This aspect is also a confirmation that the security of this service is particularly important. At the same time, each of these global players is seeking to provide its users with a stable interference positioning service, resistant to attacks of all kinds, as far as possible, such as: USA, Russia, China, Japan, India and the European Union, tests and implements satellites to develop their own positioning capabilities.

This is a major change of world configuration for the United States, which for decades has practically held the monopoly over the location determination service through the Global

[1] Gartner Says Global Smartphone Sales Continued to Decline in Second Quarter of 2019, EGHAM, U.K., August 27, 2019.

Positioning System (GPS)[2], a military service of the Air Force built during the Cold War and which subsequently allowed wider access for commercial use[3].

Owning GPS systems has a number of advantages. One of these is the fact that commercial and military users worldwide depend on this service. As a single provider, the service may be subject to restrictions, resulting in unavailability or non-compliance. Therefore, the development of technology and the put in place of new geostationary satellites systems, offer relatively viable alternatives to the general public, because they are also managed by different government entities.

Current GPS systems

For now, several world-wide systems are fully or partially operational: US- GNSS, Russia-GLONASS, China - BeiDou, EU - Galileo, Japan - QZSS, India - IRNSS, according to the table below:

Table 1. Satellite positioning systems

Owner	Acronym	Number of satellites in the system	Operational satellites
US	GPS	33	31
Russia	Glonass[4]	28	22
China	BeiDou	48	35
EU	Galileo[5]	26	26
India	IRNSS	7	?
Japan	QZSS[6]	4	4

The dependence on a single positioning service provider has been reduced, by developing these coverage systems, even partially worldwide. As an immediate effect, smart phone manufacturers have incorporated receivers compatible with same receiver of position for different systems: GPS, GLONASS, GALILEO, BeiDou. As a result, we would be tempted to conclude that the vulnerabilities generated by the positioning service are diminished. It is partially true even if we have diversified the location of the providers of location services, there are situations where the signal is not available, such as: screened spaces / locations or the signal is intentionally blocked / jammed. These aspects are translated into vulnerabilities.

Vulnerabilities of providing positioning services

The vulnerabilities generated by the existence of a single provider were solved, by extending the number of localization service providers, by developing and operating the localization systems mentioned above. The vulnerability generated by the absence or alteration of the location service remains, regardless of its provider[7].

[2] US Global Positioning System (GPS), https://www.gps.gov/systems/gps/, vizited 12.01.2019

[3] GPS: The Global Positioning System A global public service brought to you by the U.S. government, https://www.gps.gov/

[4] https://www.glonass-iac.ru/en/GLONASS/

[5] Galileo- https://galileognss.eu/

[6] QZSS - https://qzss.go.jp/en/technical/qzssinfo/index.html

[7] https://www.gps.gov/support/user/

There is enough information about GPS interruption / malfunction events with the longest operating period[8] to allow us to conclude that the availability of this type of service presents vulnerabilities. Their impact is propagated both in the economic environment, mainly in the areas related to transport (air, sea and land), military but also the social system up to the level of persons. It is important in everyday life that the localization service operates in normal parameters, is stable and precise.

If we refer to effects on social life, the following effects can be listed:

- disruption of any positioning and navigation application on the map[9] (vehicles of any type[10] [11], highlighting personal location, tourist information, etc.);
- negative effects on the systems of locating the persons and their goods in case of emergencies (medical emergencies, disappearances of people, disasters, illicit actions on the integrity of the persons and their goods, etc.).

Alternative location services to global ones

Limitations and the multitude of events that have occurred especially in the last 10 years on the actual positioning systems, the scientific and economic community have developed a series of alternative technical solutions to the current ones, given the vulnerabilities of the existing localization systems. In this sense we can highlight the solutions based on the technologies:

- Wi-Fi, Cellular, Ultra-Wideband: PhasorLab[12], Skyhook Technologys[13];
- Fiber Network: OPNT Global Terrestrial Timing Service (GTTS)[14], Seven Solution[15];
- eLORAN (Long Range Navigation): Hellen Systems[16], UrsaNav[17];
- Satellite: GlobalStar-Echo Ridge (Augmented Positioning System (APS)[18], Satelles (Iridium constellations)[19]
- Others: TRX Systems[20], NextNav[21]

All of these systems have been developed as alternatives to the classic GPS system, given its limitations. Obviously, these also have their own constraints and operating limits, but they are viable alternatives that complement the problem of localization and are mainly addressed to government institutions or organizations and less to people.

Each of the above alternatives has both advantages and disadvantages. The way of implementation and use requires costs, which for individuals are prohibitive. One of these systems is based on permanently ensuring the user's connection to it and in addition it is necessary to contribute to the development or access to the knowledge base of the service

[8] https://navcen.uscg.gov/?Do=GPSReportStatus

[9] Judah Ari Gross, *Moscow blamed for disruption of GPS systems at Ben Gurion Airport*, june 27, 2019, https://www.timesofisrael.com/moscow-blamed-for-disruption-of-gps-systems-at-ben-gurion-airport/

[10] GPS Disruptions Reported in Mediterranean Sea, https://www.satellesinc.com/gps-disruptions-reported-in-mediterranean-sea/

[11] Shipping Industry Faces GPS Disruption in Persian Gulf, https://www.satellesinc.com/shipping-industry-faces-gps-jamming-in-persian-gulf/

[12] https://www.phasorlab.com/

[13] https://www.skyhook.com/

[14] https://www.opnt.nl/

[15] https://sevensols.com/

[16] http://www.hellensystems.com/

[17] https://www.ursanav.com/

[18] https://www.echoridgenet.com/

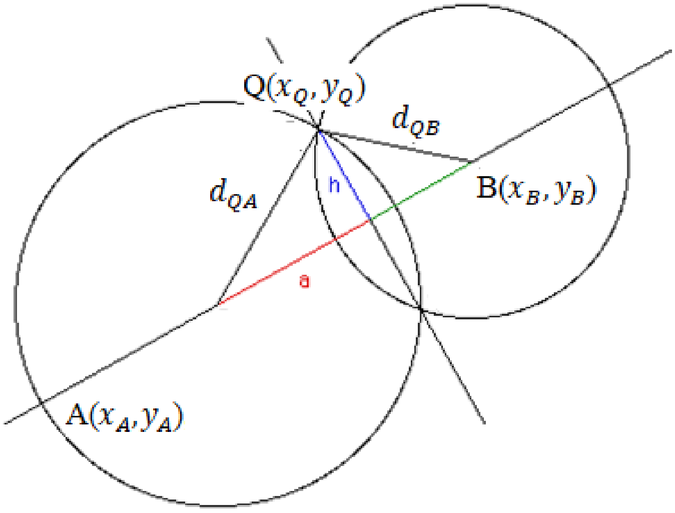
[19] https://www.satellesinc.com/

[20] https://www.trxsystems.com/

[21] https://www.nextnav.com/

provider, i.e. the locations of access points, Wi-Fi, mobile phones, etc., located in the route that he goes, obviously assumed by the user. In the absence of this pre-existing information in the database it is almost impossible to locate, as an alternative to GPS.

The determination of the current position of the mobile phone consists in determining the intersection of two circles, in which the distances to their centers represent the distance of the receiver to the two access points, respectively A(x_A, y_A), B(x_B, y_B) and d_{QA}, d_{QB}. The distance from user to the access points can be determined based on the signal strength received by the Wi-Fi interface.



[22]

Figure 1. The position of the mobile WiFi receiver - Q(x_Q, y_Q)

$$x_Q = x_A + \frac{1}{\sqrt{(x_A - x_B)^2 + (y_A - y_B)^2}} \left[\frac{{d_{QA}}^2 - {d_{QB}}^2 + (x_A - x_B)^2 + (y_A - y_B)^2}{2 \cdot \sqrt{(x_A - x_B)^2 + (y_A - y_B)^2}} \cdot (x_B - x_A) \right.$$

$$\left. + \sqrt{{d_{QA}}^2 - \frac{\left({d_{QA}}^2 - {d_{QB}}^2 + {d_{AB}}^2\right)^2}{4 \cdot (x_A - x_B)^2 + (y_A - y_B)^2}} \cdot (y_B - y_A) \right]$$

$$y_Q = y_A + \frac{1}{\sqrt{(x_A - x_B)^2 + (y_A - y_B)^2}} \left[\frac{{d_{QA}}^2 - {d_{QB}}^2 + (x_A - x_B)^2 + (y_A - y_B)^2}{2 \cdot \sqrt{(x_A - x_B)^2 + (y_A - y_B)^2}} \cdot (y_B - x_A) \right.$$

$$\left. - \sqrt{{d_{QA}}^2 - \frac{\left({d_{QA}}^2 - {d_{QB}}^2 + {d_{AB}}^2\right)^2}{4 \cdot (x_A - x_B)^2 + (y_A - y_B)^2}} \cdot (x_B - x_A) \right]$$

InCity Positioning Application

A simple application can be implemented, which will locally manage the information database of these access points, in order to eliminate the need for the user with position information of the access points to the service provider with the ability to determine the location using information provided by the WiFi access points. The database will store the location information from the person's route, being completely under his control. In certain situations, it can transmit the location by text messages to correspondents previously

[22] http://mathworld.wolfram.com/Circle-CircleIntersection.html

established. The user will be able to build his database, stored locally, and will be able to exploit the location first-hand, in the absence of the classic GPS signal. Of course, this solution has the disadvantage that it cannot determine the location in an area that has not been previously recorded the coordinates of the access points.

For this, the local database must stored at least the following information about WiFi access points: *ssid* - network name; *bssid* - the physical address of the access point; *capabilities* - authentication data, keys, encryption scheme; *level* - the level of the signal expressed in dBm; *dist* - the distance to the access point; *timestamp* - the time stamp at which the data were recorded, as follows:

```
{"AccessPoint":
        [{"ssid":"AP1","bssid":"00:00:00:aa:bb:cc", "latitude":45.010101,
          "longitude":28.010101, "capabilities":"[WPA2-PSK-CCMP][WPS][ESS]",  "level":-
6,"dist":0.2}] }
```

Considering the above, we define a protocol for determining the location in the absence of GPS signal, Offline In-City Positioning - OffICPos, as follows:

```
OffICPos ( AccesPoints, timestamp)
        a)  learningPhase ()
                - acquire data (timestamp)
                        accesPoints and its parameters
                - register to Database (timestamp)
                        [{"ssid":"$x_1$","bssid":"$y_1$", "latitude":$w_1$, "longitude":$z_1$}, ...
                         {"ssid":"$x_n$,"bssid":"$y_n$", "latitude":$w_n$,        "longitude":$z_n$}]

        b)  offline GPS ()
                - scanningData (timestamp)
                        return near currentAccesPoints
                - interogateDatabase (currentAccessPoints)
                        return  databaseAccesPoint
                        [{"ssid":"x","bssid":"y", "latitude":y,  "longitude":z }]

        c)  sendSOSMessage ()
                - send text message(x,y) to main lists with near acces point and its
                  coordinates.
```

If we admit that the error in determining the location is up to 10 meters, we can say that the offline GPS location corresponds to the nearest AccessPoint, within the error limit.
We performed a data acquisition experiment of a set, on an area of 0.25 square kilometer, identifying a number of over 800 access points, resulting in an average density of about 3000 access points per square kilometer, which ensures a sufficiently large number to determine the location with an acceptable error.

Such a solution is useful, both for its own use, but it can also be implemented at the organizational or governmental level, to complete the localization system in case of GPS service or Internet connection unavailability.

BIBLIOGRAPHY

1. Mark Sullivan, *A brief history of GPS,* https://www.pcworld.com/article/2000276/a-brief-history-of-gps.html, last visited 01.10.2018
2. Richard B. Langley, *Innovation: GLONASS — past, present and future,* November 1, 2017, https://www.gpsworld.com/innovation-glonass-past-present-and-future/
3. Indian Regional Navigation Satelite System, https://www.isro.gov.in/sites/default/files/irnss_sps_icd_version1.1-2017.pdf

4. Danny Crichton, Arman Tabatabai, *The GPS war begun*, December 21, 2018, https://techcrunch.com/2018/12/21/the-gps-wars-have-begun/
5. *True Stories of GPS Tracking Saving Children's Lives*, https://thriveglobal.com/stories/5-true-stories-of-gps-tracking-saving-children-s-lives/
6. Dana Goward, *GPS backup demonstration projects explained*, January 9, 2020, https://www.gpsworld.com/gps-backup-demonstration-projects-explained/
7. *No GPS, no problem: Next-generation navigation*, https://www.sciencedaily.com/releases/2016/10/161013150039.htm
8. Sandra Erwin, *No GPS? No problem, there are increasingly more options*, July 24,2018 https://spacenews.com/no-gps-no-problem-there-are-increasingly-more-options/
9. Elisabeth Braw, *The GPS war are here*, December 17, 2018, https://foreignpolicy.com/2018/12/17/the-gps-wars-are-here/

ARTIFICIAL INTELLIGENCE AND COMBAT VEHICLES

Adrian STANCIU
PhD. Candidate, “Carol I” National Defence University, Panduri Street, Bucharest, Romania,
stanciuady@gmail.com

Abstract: *The use of Artificial Intelligence (AI) that is integrated into Military Combat Systems, is a new approach for not only current but future warfare. In doing so, this potentially will reduce the response time and human inaccuracy during combat operations. AI integration will be able to receive, process and eliminate threats faster, which will increase safety for Military Personnel and Equipment.*

Keywords: *artificial intelligence, combat vehicles, combat operations, battlefield.*

In our daily activities artificial intelligence has become a part of our lives. We can list examples of using AI in today’s technologies like: automatic translations, robots, chess programs, medical diagnostics, automatic planning, finding the optimal routes, smart phones, drones, smart cars, optical character recognition, voice, face activation and smart devices for house.

Furthermore AI has become an important element of modern warfare, because it can improve self-control, self-regulation and self-actualization of combat systems due to its fundamental automated and decision-making capabilities.[1] Dr. Daphne Richemond-Barack[2] stated in a conference at the Herzlya Interdisciplinary Center, Israel, that artificial intelligence has the capacity to increase the speed of conventional warfare. AI systems have the possibility to include the capabilities of smart combat systems, using enormous sums of field data more efficiently and replacing humans.

The artificial intelligence refers to systems or machines that imitate the human intelligence, to perform various activities and which can be improved continuously based on the information they collect.[3]

At the opening of the international conference “International Armored Vehicles”, in London, in 21-22.01.2020, General Adrian Bradshaw (former Deputy Supreme Allied Commander Europe, in March 2014-March 2017) mentioned that in the battle field new and complex challenges are emerging, such as aggression between states, energy and climate crises, global terrorism, which are only part of the new threats, so we must remodel the future actions. It is very important to see the global threats enter the realm of physical and digital and national security must prepare for future challenges.[4]

In the modern battlefield artificial intelligence learns along with the operators how to take control of fire systems and logistics.

The new systems that integrate AI allow operators to focus on the most important tasks, not to consume energy performing simple and repetitive operations such as driving a

[1] Heba Soffar, Military Artificial Intelligence (Military Robots) Advantages, Disadvantages & Applications, Robotics Site, accessed February 21, 20, on https://www.online-sciences.com/robotics/military-artificial-intelligence-military-robots-advantages-disadvantages-applications /

[2] Assistant Professor at the Lauder School of Government, Diplomacy, and Strategy at IDC Herzliya, and a Senior Researcher at INSCT partner organization the *International* Institute for Counter-Terrorism (ICT).

[3] https://www.oracle.com/ke/artificial-intelligence/what-is-artificial-intelligence.html, accessed February 21, 20

[4] Reflections on International Armoured Vehicles 2020 Part 1, accessed on February 02, 20 on https://www.defenceiq.com/armoured-vehicles/editorials/armoured-innovation-reflections-on-iav-2020-part-1.

vehicle or loading the fire systems with munitions. These systems that can be trained, taught and able to decide independently will probably dominate the AI domain.

The AI is used by the great powers, such as USA, Russia, and China and among others, in the creation and development of a new weapon systems, air, and navy, ground platforms that can partially or totally replace the systems where man has a big influence on them. Military artificial intelligence allows the development of effective combat systems based more or less on human actions. These systems become a decisive part of modern war, as they improve the control of combat vehicles in difficult situations, ensure a better accuracy of fire systems due to the observation systems of the battlefield, identification and tracking targets, find the distance to them, identifies the ammunition with which the target can be destroyed, identifies the action possibilities and the decision to execute the shot.[5]

In the defence and military areas AI is used today by military and intelligence organizations from around the world to maximize the capabilities of AI in these areas.

The military and defence organizations can use AI for:

- Fire systems automatization;
- Surveillance;
- Cybernetic security;
- Interior security;
- Autonomous vehicles.[6]

AI is used in military applications because it can collect a lot of information from sensors (such smart phones, video cameras, computers, surveillance and reconnaissance devices, UAVs and satellites). The military organization can observe the increase in the surveillance and reconnaissance quality's due to removing the human factors in process of sensors operations.

Machine learning ability, observation and data dissemination through software can be used for surveillance operations by being capable of sorting out huge amounts of information faster than human analysts.

Autonomous weapons systems are using software to identify and track targets but can't fire upon without a human who is monitoring the system.

Autonomous combat vehicles increase operator productivity and protection. It can patrol with disregard to terrain and weather and provide oversight over the areas to alert personnel about breaches. With the help of these vehicles it can reduce significantly the need for patrol personnel. The AI is also used for logistics convoys for supply, ammunition weapons and personnel transportation. AI will significantly reduce transportation costs, human resources, and human errors (mistakes associated with fatigue, stress and routine) during operations. It also can be used to predict and detect beforehand potential malfunctions of autonomous combat vehicles. By using artificial intelligence during operations, you can track with high accuracy the designated targets within a complex conflict area which can help the people in command identify potential future operations areas through analysis of reports, documents, news feeds and all information that AI can track from open sources.

To have a better understanding of the importance of using artificial intelligence in military operations I'm going to discuss new technological trends which can be used on combat vehicles in near future.

[5] Heba Soffar, *Military Artificial Intelligence (Military robots) advantages, disadvantages & applications*, Robotics, 29.08.2019,accessed January 31, 20, on https://www.online-sciences.com/robotics/military-artificial-intelligence-military-robots-advantages-disadvantages-applications/

[6] Marcus Roth, Emerj, *Artificial Intelligence in the Military – An Overview of Capabilities,* accessed February 04, 20, on https://emerj.com/ai-sector-overviews/artificial-intelligence-in-the-military-an-overview-of-capabilities/

First, I will describe the Carmel program with is developed by Israel and that involves artificial intelligence in new military technologies that will reduce collateral damage and enable autonomous unmanned vehicles working in concert.

The director of Research and Development department Brigadier General Yavin Rotem, stated in an interview for Defence News the Carmel program is revolutionary and has been in development for several years. Using artificial intelligence will reduce the number of soldiers inside of vehicles from the usual four to two, will enhance vehicle performance, all in a closed cockpit or turret. The system is using the latest optical and acoustic technologies to allow maneuverability and a 360-degree view. [7] They also are trying to implement new technologies on existing platforms, such as Merkava, Eitan and Namer. They are also trying to use sensors to identify small targets (mini vehicles, small drone, and so on) allowing the platform based on artificial intelligence to be autonomous, to identify and provide to military personnel the most effective routes, places to camp and POT.

The new battlefield challenge for combat vehicles will be the ability to detect and identify threats, some of them hidden among civilians or in their homes. Artificial intelligence will be able to detect potential targets, to analyze information and decide which of them are threats.

The Israeli companies which develop programs for military vehicles are using artificial intelligence along with 360^0 technology dispersed on a formation of military vehicles, with or without a crew. These are executing combat missions together, identifying the threats and sharing at the same time the same information about battlefield with the purpose of selecting the best way to neutralize the threat. Let’s imagine that one military vehicle is illuminated in spotlight by an anti-tank team, a second and third vehicle have a better view on this team, and the both vehicles can use their weapon systems to annihilate the anti-tank team. While two soldiers have the mission to lead and use the weapon system, the third soldier has the possibility of coordinating the vehicles, maybe from a mobile command point, from the back. Simultaneously Israel wants their future battle vehicles to have hybrid propulsion and low footprint.

Picture Iron Vision Helmet[8]

Israel Aerospace Industries (IAI) and Rafael Advanced Systems build a simulator, which will imitate the interior of an armored vehicle. Inside this simulator using a crew of two soldiers, meanwhile on the panoramic screens it displays a battlefield scenario, like an urban area owned by Hezbollah. The crew was equipped with headphones with screen (Elbit

[7] Seth Frantzman, *Israel’s Carmel program: Envisioning armored vehicles of the future*, accessed on February 10, 20, on https://www.c4isrnet.com/artificial-intelligence/2019/08/05/israels-carmel-program-envisioning-armored-vehicles-of-the-future/

[8] Barbara Opall-Rome, *IronVision Helmet Provides Sight Through Armored Tanks,* Defence News, accessed February 15, 20, on https://www.defensenews.com/land/2016/06/08/ironvision-helmet-provides-sight-through-armored-tanks/

System's Iron Vision Helmet Mounted Display[9]) and a joystick. The Iron Vision helmet offers a 360^0 overview of the battlefield through the 40 cameras mounted on the outside of the vehicle. This equipment was tested on vehicles in four different scenarios during day and night. General Rotem pointed out the fact that those tests changed the way of thinking about using land forces in ground actions. At the same time, he pointed out that artificial intelligence, autonomous capabilities and the multitude of sensors, together will change the combat vehicles course of actions in the battlefield.

Israel uses the technology developed through this program to modernize its existing combat vehicles, as well as to develop a new combat vehicle platform. In cooperation with the USA, Israel also is developing the Trophy[10] program, in which artificial intelligence is used for combat vehicles close in protection.

The second possibility for use of AI on combat vehicles, the reporter Aaron Gregg published an article in The Washington Post daily paper about "Army to use artificial intelligence to predict which vehicles will break down"[11], in which he presents how AI can assist the US army to identify in a timely manner the military vehicles equipment which are damaged during combat missions.

Chicago-based Uptake Technologies Company has signed a contract with the US Army for testing the company's AI technology on several Bradley M2A3 before implementing the new technology on the entire Bradley fleet. Lieutenant-colonel Chris Conley, the Bradley program manager, stated that he needs to see if some of the Uptake's machine learning algorithms can be used to detect the equipment malfunctions before it fails. For example, if the equipment shows signs of failure, vehicle operators will be warned and will have the opportunity to repair or replace equipment before the entire vehicle will be out of order.[12] If these algorithms can be implemented, then the US Army will extend this program to the entire Bradley platform as well as other combat vehicles.

Another example for using the AI on future combat vehicles was describe by Margareta Konaev and Samuel Bendett in 2019, an "Russian AI-enabled combat: Coming to a city near you?" article, the Russian army sees military artificial intelligence as a facilitator for its automated command systems and supports the decision-making process by faster analysis of multitudes of data from different domains. The Russian Ministry of Defence wants to develop AI for performing the operations likes human brain functions. Equipping autonomous or semi-autonomous ground, naval, aerial, military vehicles with AI will improve force protection, to understand deeper the battlefield situation, ensuring the maneuvers and freedom of movement on any area or weather.

Russian Chief of Staff General Valery Gerasimov sees the battlefield in Syria like a sum of modern war scenarios and, he told the Russian army will be investing in military technology and it will improve their tactics. In his vision Syria presents the "contours of future war"[13]- another combat type which involves military robots, unmanned vehicles,

[9] https://elbitsystems.com/pr-new/elbit-systems-introduces-ironvision-helmet-mounted-system-armored-fighting-vehicles/, accessed February 15, 20.

[10] The program developed by the Israel army that uses an active protection system for intercepting and destroying projectiles, missiles, rockets fired on combat vehicles equipped with this system.

[11]Aaron Gregg, Army to use artificial intelligence to predict which vehicles will break down, June 26, 2018, accessed January 26, 20, on https://www.washingtonpost.com/business/capitalbusiness/army-to-use-artificial-intelligence-to-predict-which-vehicles-will-break-down/2018/06/25/bfa1ef34-789f-11e8-93cc-6d3beccdd7a3_story.html

[12] Victoria Leoni, Here's how artificial intelligence could predict when your Army vehicle will break down, ArmyTimes, accessed February 15, 20 on https://www.armytimes.com/news/your-army/2018/06/27/heres-how-artificial-intelligence-could-predict-when-your-army-vehicle-will-break-down/

[13] Margarita Konaev şi Samuel Bendett, Russian AI-Enabled Combat: Coming to a City Near You?, War on the Rocks, accessed February 15, 20, on https://warontherocks.com/2019/07/russian-ai-enabled-combat-coming-to-a-city-near-you/

precision – guided munitions, and robust C4ISR[14] as well as information operations. The Russian army argues they have this type of equipment and - it was used in Syria – and other technologies already have been tested in urban conditions or may be applicable for urban combat.

Furthermore, in Syria the Russian forces tested several versions of unmanned combat vehicles with different missions like mine clearance, intelligence, surveillance, reconnaissance (ISR), logistics and combat missions. To reduce personnel and technical losses in ISR missions, they are use small vehicles such Scarab[15], Sphere (small unmanned vehicles for ISR)[16], Ural-6[17]. The Ural-6 unmanned vehicle demining systems were deployed by the Russian troops for the removal of explosive devices in Palmyra, Siria, in April 2016.[18] The Nerehta, the Armed Unmanned Ground Vehicle is a vehicle with a lot of possibilities for use in the battlefield. It is a small vehicle, with 0 crew members, which has been developed to be for multirole functions, like: reconnaissance, artillery spotting/support, troop-carrying, utility, and basic infantry fire support. The AI implemented on this platform provides the reconnaissance along with an aerial drone and fire support. It features a computer-controlled system, protected communication channel, and various sensors. It can operate autonomously, select target son its own, and can be commanded in manual mode from a distance of up to 5 km. The vehicles are manufactured in Russia by the Degtyarev Plant and add an interesting element within existing modern Russian infantry doctrine.

As a conclusion we can say there will be in advantage the army will be able to use AI in combat vehicles, because it will reduce the loss of human life and materials. Furthermore, it will decrease the costs for equipment and training the troops. The combat vehicles that are include AI can function anywhere, in any conditions, and it can remove the human factor and improve the accuracy of reconnaissance and fire systems. Also, it will increase crew safety while the costs of repairs will decrease by performing an efficient maintenance program. All the information about all the on-board system's equipment in future combat vehicles will be automatically stored, analyzed and used with AI to improve the techniques.

BIBLIOGRAPHY:

1. Aaron Gregg, Army to use artificial intelligence to predict which vehicles will break down, June 26, 2018, on https://www.washingtonpost.com/business/capitalbusiness/army-to-use-artificial-intelligence-to-predict-which-vehicles-will-break-down/2018/06/25/bfa1ef34-789f-11e8-93cc-6d3beccdd7a3_story.html
2. Barbara Opall-Rome, IronVision Helmet Provides Sight Through Armored Tanks, Defence News, on https://www.defencenews.com/land/2016/06/08/ironvision-helmet-provides-sight-through-armored-tanks/

[14] Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

[15] The small, remote controlled device is equipped with high resolution and thermal imaging cameras which allows Russian troops to safely inspect confined areas for explosive booby traps and waiting ambushes. The ongoing modernization effort of the Russian military includes several armed and unarmed robots of various size, built for differing mission types; accessed February 24, 20, on https://www.funker530.com/russian-de-mining-robots/

[16] Samuel Bendett, "Russia Is Poised to Surprise the US in Battlefield Robotics", accessed February 25, 20, on https://www.defenseone.com/ideas/2018/01/russia-poised-surprise-us-battlefield-robotics/145439/

[17] Uran-6 is a multi-functional, mine-clearing robotic system manufactured by JSC 766 UPTK for the Armed Forces of the Russian Federation., accessed on February 24, 20, on https://www.army-technology.com/projects/uran-6-mine-clearing-robot/;

[18] Staff Writer, Nerehta AUGV, Military factory, 12.09.2018, accessed February 25, 20, on https://www.militaryfactory.com/armor/detail.asp?armor_id=1139;

3. Heba Soffar, Military Artificial Intelligence (Military Robots) Advantages, Disadvantages & Applications, Robotics Site, on https://www.online-sciences.com/robotics/military-artificial-intelligence-military-robots-advantages-disadvantages-applications /
4. Marcus Roth, Emerj, Artificial Intelligence in the Military – An Overview of Capabilities, on https://emerj.com/ai-sector-overviews/artificial-intelligence-in-the-military-an-overview-of-capabilities/
5. Margarita Konaev şi Samuel Bendett, Russian AI-Enabled Combat: Coming to a City Near You?, War on the Rocks, on https://warontherocks.com/2019/07/russian-ai-enabled-combat-coming-to-a-city-near-you/
6. Samuel Bendett, "Russia Is Poised to Surprise the US in Battlefield Robotics", on https://www.defenceone.com/ideas/2018/01/russia-poised-surprise-us-battlefield-robotics/145439/
7. Seth Frantzman, Israel's Carmel program: Envisioning armored vehicles of the future, accessed on https://www.c4isrnet.com/artificial-intelligence/2019/08/05/israels-carmel-program-envisioning-armored-vehicles-of-the-future/
8. Staff Writer, Nerehta AUGV, Military factory, 12.09.2018, on https://www.militaryfactory.com/armor/detail.asp?armor_id=1139
9. Victoria Leoni, Here's how artificial intelligence could predict when your Army vehicle will break down, ArmyTimes, on https://www.armytimes.com/news/your-army/2018/06/27/heres-how-artificial-intelligence-could-predict-when-your-army-vehicle-will-break-down/
10. ***Reflections on International Armoured Vehicles 2020 Part 1, on https://www.defenceiq.com/armoured-vehicles/editorials/armoured-innovation-reflections-on-iav-2020-part-1
11. https://www.army-technology.com/projects/uran-6-mine-clearing-robot/;
12. https://elbitsystems.com/pr-new/elbit-systems-introduces-ironvision-helmet-mounted-system-armored-fighting-vehicles/
13. https://www.funker530.com/russian-de-mining-robots/

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON CYBER SECURITY

Marius COSTACHE
Master Student, "Carol I" National Defence University,
mcostache@mapn.ro

***Abstract**: The technology evolved so quickly that it led to the inclusion of artificial intelligence in the process of securing the cyber environment. Both the private and the military sectors are interested in understanding and using artificial intelligence for data protection and for creating more opportunities that can improve specific activities. Taking into consideration the technology progress, there are some cyber-security companies on the market that developed artificial intelligence solutions based in order to protect against cyber-attacks. The products that were developed using artificial intelligence support the cyber security specialists to identify and investigate some complex cyber threats, such as advanced persistent threat campaigns. The military forces will face serious challenges in order to maintain operational cyber infrastructures, although in many areas, they could benefit from using artificial intelligence for security purposes.*

***Keywords**: artificial intelligence, cyber space, APT, cyber security, machine learning.*

The technology evolved so quickly that it led to the inclusion of artificial intelligence in the process of securing the cyber environment. Both the private and the military sectors are interested in understanding and using artificial intelligence for data protection and for creating more opportunities that can improve specific activities[1].

In the field of cyber security, there is a consensus on the following: *The change* is continuous. The specialists should permanently review what they did yesterday and identify what needs to be improved. In order to keep up with our opponents, we must improve the way we operate and apply new technologies, so that we can find better solutions to defend or prevent an attack. In short, if we will not be able to learn and constantly improve our protection systems, we will not be able to maintain our security system to an acceptable risk level.

Many companies in the field of information technology have invested, lately, huge financial funds, for the development of cyber security systems based on artificial intelligence, machine learning and deep learning for protection against cyber attacks.

Modern technologies such as artificial intelligence, machine learning, deep learning, have become the key words that everyone talks about in response to the current market opportunities, but nobody fully understands what that is. All of these terms seem very complicated in the beginning. There is a misconception about words, because most of the people believe that these things are the same as directly related to machine learning or artificial intelligence.

In order to give a real meaning to these terms which I will operate with, I will try to give a definition of what artificial intelligence represents and what is the relationship with machine learning and deep learning.

Artificial Intelligence (AI) is a branch of computer science that is seeking to build intelligent machines that are programmed to think like humans and mimic their actions.

[1] *Buletin CYBERINT*, Semestrul I-2019, accessed February 20, 2020, on https://www.sri.ro/assets/files /publicatii/buletin-cyber-sem-1-2019.pdf

Machine learning (ML) is a branch of artificial intelligence science that aims to give machines the ability to „learn”. This thing is done by using algorithms that identify models based on the data received, so that the machines can take decisions and make predictions, meaning they become „intelligent”. This way it is no longer necessary for the machine to be specifically programmed for each action.

Deep learning (DL), on the other hand, is a subset of machine learning that represents the most advanced field of artificial intelligence. It has the main objective of giving machines the opportunity to „learn” and „think” very similar with the people.

The relationships between the three elements are shown in Figure 1.

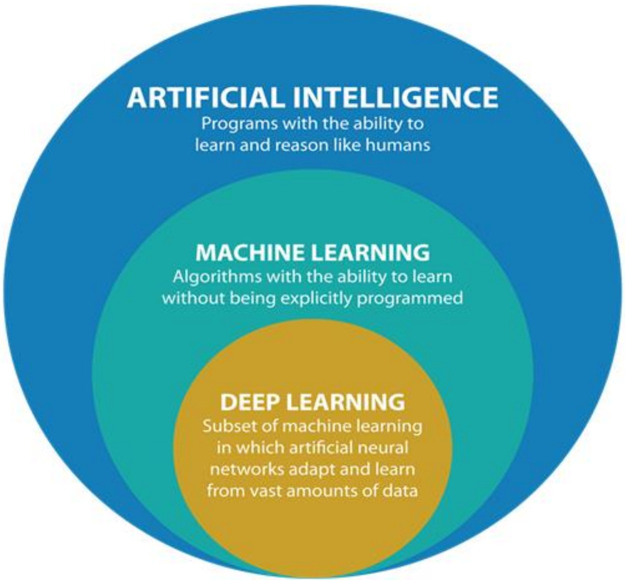

ARTIFICIAL INTELLIGENCE
Programs with the ability to learn and reason like humans
MACHINE LEARNING
Algorithms with the ability to learn without being explicitly programmed
DEEP LEARNING
Subset of machine learning in which artificial neural networks adapt and learn from vast amounts of data

Figure 1. Relation between AI, machine learning and deep learning[2]

If we are talking about security systems based on AI, we will have to point out that they are different from the classical security systems in the sense that they are not programmed but they are constantly learning how to act.

Cyber security specialists must deal with much better organized attackers, who have access to important resources and are often supported by terrorist organizations or even state actors. In front of these increasingly complex threats, traditional security systems have two major weaknesses.

The first of these is the fact that they are rely on strict rules, being programmed based on an understanding of the existing threats, some threats that cyber specialists have faced and eliminated. The biggest problem is that the current threats have evolved considerably in volume and complexity. The attackers have evolved their attack tools, the malware used by them being in a continuous change.

The second shortcoming of the classic security systems is their inability to scale to the size of modern organizations. If we are to consider the complexity of the current business environment, forced to combine the old technology with the modern technology, but also the fact that they need to expand their connections outside the organization, we will realize that doing basic things such as sanitation, patching, vulnerability management to find out there the weaknesses of the security system, is an extremely complex thing and will be very difficult to put into practice if we take into account the rapid pace of the organization evolution.

[2] https://www.argility.com/argility-ecosystem-solutions/iot/machine-learning-deep-learning/, accessed February 19, 2020.

The existing solutions which are using old engines are already outdated, attackers adapting to the new technologies. These old solutions can test files before they are executed, in many cases the threat already being in the systems that should be protected, often the simple blocking of file execution being already a late measure. High-precision system learning activates advanced security features, completely blocking the attacks and removing them from the system, but also blocking fake file entries, as well as exploitation of operating systems to be broken.

In cyber security, machine learning activates advanced software security systems, which easily and quickly are recognizing threats that attack systems, blocking them altogether. Meanwhile, a threat database is automatically being built, helping applications to block attacks more efficiently over time.

That is why it is necessary the evolution to the next generation of security systems based on artificial intelligence and machine learning. These will not be programmed around a threat, but they will have a pattern, they will try to learn on the job what is good and how to act, thus automatically responding to the user's security needs.

Through artificial intelligence, machine learning and cyber threat information, the organizations can respond to threats with enhanced confidence and increased speed.

Furthermore, I will present some of the advantages of using artificial intelligence in cyber security.

Automatic detection

AI has led to smarter automated security measures, and with the help of machine learning, AI software can detect threats and correlate potential risks without being asked. This level of detection means that the monotony of threat detection is not led by man, which automatically results in fewer human errors.

Due to machine learning, AI can learn by experience and pattern, rather than by cause and effect. Currently, machine learning allows machines to learn on their own. This means that they can build models for patterns recognition, rather than relying on people to build them.

One of the most widely used methods of cyber attack, in which hackers try to deliver their malware using techniques to manipulate the identity data of a person or institution is phishing. Phishing emails are extremely widespread; one of 99 emails are a phishing attack. Fortunately, AI-ML can play a significant role in preventing and discouraging phishing attacks.

AI-ML can detect and track more than 10000 active phishing sources and react/remediate much faster than people can. AI-ML is also working on scanning phishing threats around the world and there is no restriction on understanding phishing campaigns in any specific geographical area.

AI has made it possible to quickly differentiate between a fake site and a legitimate one.

The AI is well-trained to consume large amounts of data, such as blogs and news, which means it has a better understanding of cyber security threats. From there, Artificial intelligence in cyber security uses patterns to identify threats (strange files, suspicious addresses, etc.) before launching a response to a legitimate threat.

Error-free cyber security

As I mentioned earlier, AI and machine learning reduce the risk of human error. People can get tired and become bored when performing monotonous tasks; AI - no. Security teams strive to act with the weight of all the data needed for the risk assessment, but AI can quickly discern all threatening factors. Nevertheless, AI and human intelligence must work together. In addition, human experts offer the common sense that machines do not have, and they are doing a better job when it comes to taking decisions.

As it is known, the decisions can be taken institutionally and/or individually. Being a member country of the European Union, we have the obligation that in the field of cyber security to harmonize and adapt the relevant legislation as well as the implementing measures[3].

This is not easy to be done because „Cyber defence is not defined within EU documents, taking into consideration the sensitivity among the member states on this issue as well as the reluctance of certain member states to participate to this action, considering their own cyber defence strategies.

This is also the reason why cyber defence, contrary to cyber-crime and NIS (*Network and Information Security*), it falls under the intergovernmental mandate of Common Security and Defence Policy – CSDP and not within the exclusive or shared competence of the EU"[4].

Faster response times

With an overwhelming amount of data to interact with, it is no wonder that it takes more time for people to go through and distinguish between threats and risks. AI is a powerful tool. AI processes large amounts of unstructured information in a coherent whole, leading to greater efficiency.

In addition, machine learning means that AI can learn patterns much faster than humans. These speeds up the response time, making it easier and faster to stop threats before they cause problems. A significant number of companies offering cyber security solutions are now applying AI and cognitive technologies in cyber security space, to enable organizations to identify threats more quickly and respond them more effectively.

Limitations of AI use in cyber security

The advantages presented above are just a part of the potential of AI to help cyber security, but there are also some limitations that prevent AI from becoming a major tool used in the field. In order to build and maintain AI – based systems, companies would require a huge amount of resources including memory, data and computing power. In addition, because AI systems are trained by learning the data, cyber security companies must provide several different databases of malware, non – harmful codes and anomalies. Obtaining all these precise databases can take a lot of time and resources, which some companies cannot afford.

Another disadvantage is that hackers can use AI themselves to test their malware and to improve it, to become AI resistant. In fact, a malware that is based on AI can be extremely destructive, as it can learn from existing AI tools and can develop more advanced attacks in order to infiltrate the traditional cyber security programs or even AI systems.

Knowing these limitations and disadvantages, it is obvious that AI is far from becoming the only cyber security solution. Meanwhile, the best approach would be to combine traditional techniques with AI tools, so that organizations should take these solutions into account when developing their cyber security strategy.

I believe that these strategies must be applied at both European and national levels. Therefore, it is appreciated that *„Improving the way the EU ensures cyber security is essential in order to continue to ensure the social, economic, financial and cultural benefits that citizens and businesses from the Internet obtain and, more broadly, the evolution of technologies for communications and information. Moreover, it is essential for the EU to achieve the goals it has set in the Digital Agenda for Europe (2010), and just as significant, the driving force of such an agenda – the Europe 2020 Strategy"*[5].

[3] D. Turcu, *Considerations on cyber security legislation and regulations in Romania*, International Scientific Conference „Strategies XXI", 2016, Vol. 3, p. 173.

[4] Col. (r.) prof. univ. dr. Gheorghe Boaru, *Securitatea cibernetică în Uniunea Europeană,* Revista Academiei de Științe ale Securității Naționale, Nr.2, 2017, p.75.

[5] *Ibidem,* p. 71.

In full agreement with the European actions, at the national level, was approved in February 2015 the *National Strategy on the Digital Agenda for Romania 2020*[6].

This strategy, „defines four areas of action, from which I only mention the first domain: e-Government, Interoperability, *Cyber Security*, Cloud Computing and Social Media. This document has taken over and adapted to our country's specific, the elements of the Digital Agenda for Europe. The Digital Agenda thus defines the major role that ICT use must play in achieving Europe 2020 objectives"[7].

The opinions of security experts are divided regarding the replacement of security specialists with computer defence systems that use artificial intelligence to counter cyber-attacks before they are detected by a person. One of the solutions may be to intensify, at institutional level but also individually, the effort to develop the security culture.

„Concepts such as „open-security", „open-society", or virtual organizations (Anonymous) are increasingly being used and attract many supporters who are active in the online environment even through cyber-aggression against security organizations.

From this point of view, the tendency to improve the culture of cyber security must natural in the society, to start from the ordinary user, as a result of the technical-scientific progress and emergence of new social values and should not be transformed into a rigid means of stopping the evolution and expansion of cyber space"[8].

The role of artificial intelligence in cyber security could be somewhere in the middle: between replacing a person with the help of artificial intelligence and helping to strengthen the network's defence measures with the help of ML.

The goal of AI is to increase human intelligence – not to replace it. There are still significant limits to what cognitive technologies can do, especially in the area of decision making, where people are able to weigh factors that cannot be easily expressed in algorithmic terms.

As technology evolves, adversaries improve their attack methods, tools and techniques to exploit individuals and organizations. There is no doubt that AI is incredibly useful but is it somehow a double-edged sword. AI-ML can be used to detect and prevent attacks before they occur, but at the same time it can be used by the attacker to perfect his attacks.AI-ML can be used to detect and prevent attacks before they occur, but at the same time it can be used by the attacker to perfect his attacks.

„If we admit the fact that a cyber space is a space where a complex confrontation can take place, with important state or non-state actors, as in the case of international terrorism or cross-border crime, then the conflict in the cyber environment, or cyber war is a phenomenon at the confluence of several forms of confrontation between these actors, as follows: imagological warfare; psychological warfare; the war of information/counter-information; cyber terrorism; network-based warfare; command and control warfare; electronic warfare; computer crime etc."[9].

Even though AI becomes more and more skillful in addressing complex security challenges, cyber attackers will seek new ways to solve or deceive its machine learning models. There is no perfect AI, but it is already a very effective and powerful security tool. As

[6] *Strategia Națională privind Agenda Digitală pentru România 2020* it was approved by HG no. 245/April 7, 2015.

[7] Col. (r.) prof. univ. dr. Gheorghe Boaru, *Securitatea cibernetică în Uniunea Europeană,* Revista Academiei de Științe ale Securității Naționale, Nr.2, 2017, p. 72.

[8] Colonel (r.) prof.univ.dr. Gheorghe Boaru, Drd. Benedictos IORGA, *Cultura de securitate – prima linie a apărării cibernetice,* Revista de Științe Militare, Editată de Academia Oamenilor de Știință din România, Nr. 2, 2015, p.142.

[9] Colonel (ret.) prof. univ. dr. Gheorghe Boaru, *Război și apărare în spațiul virtual,* Revista de Științe Militare, Editată de Academia Oamenilor de Știință din România, Nr. 2, 2018, p. 51.

they mature, security teams will integrate AI – based security software as a basic solution for cyber infrastructure protection.

While AI and automation will play a key role in releasing overloaded IT security teams, organizations will continue to require highly qualified individuals to perform high – level analysis and remediation activities – not to mention the training needed for the machine learning to be effective.

Although artificial intelligence is in the phase of redefining and discovering new ways of implementation, the entities which will benefit from this technology will gain certain advantages, both in the short and long term.

It is appreciated that „*Securing the virtual space* has become one of the most pressing security challenges of the 21st century, due to its importance for everyday life, for the government, national security, business and for the citizens alike. The cyber world and its associated technologies have created, on the one hand, more social, cultural, economic and political opportunities for all of us, but on the other hand, its borderless nature has brought with it threats in the form of cyber attacks and cybercrime”[10].

In conclusion, we can strongly affirm that we need artificial intelligence/machine learning in cyber security, but we also need people to "learn" it and use it effectively.

BIBLIOGRAPHY

1. ****HG nr. 494/2011* privind înfiinţarea *Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO.*
2. ****HG nr. 271/2013* pentru aprobarea *Strategiei de securitate cibernetică a României* şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică. Anexa nr.1 la Strategia de securitate cibernetică a României.
3. ****HG nr. 245/7 apr. 2015* prin care se aprobă *Strategia Națională privind Agenda Digitală pentru România 2020.*
4. Strategia de securitate cibernetică a României, 2013.
5. Legea privind securitatea cibernetică a României, 2014.
6. ****Cybersecurity Strategy of the European Union*, Brussels, 7.2.2013, JOIN (2013) 1 final, [http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf].
7. Max Lungarella, Fumiya Iida, Josh Bongard, Rolf Pfeifer, *50 Years of Artificial Intelligence,*Series: Lecture Notes in Artificial Intelligence, Publisher: Springer, 2008.
8. Tareq Ahram, *Advances in Artificial Intelligence, Software and Systems Engineering: Proceedings of the AHFE 2019,* Series: Advances in Intelligent Systems and Computing 965 Publisher: Springer International Publishing, 2020.
9. Timothy Leary, Michael Horowitz, Vicki Marshall, *Chaos & Cyber Culture,* Publisher: Ronin Pub, 1994.
10. Col. (r.) prof. univ. dr. Gheorghe Boaru, *Securitatea cibernetică în Uniunea Europeană*, Revista Academiei de Științe ale Securității Naționale, Nr. 2, 2017.
11. Colonel (ret.) prof. univ. dr. Gheorghe Boaru, *Război și apărare în spațiul virtual,* Revista de Științe Militare, Editată de Academia Oamenilor de Știință din România, Nr. 2, 2018.
12. Colonel (r.) prof.univ.dr. Gheorghe Boaru, drd. Benedictos Iorga, *Cultura de securitate – prima linie a apărării cibernetice*, Revista de Științe Militare, Editată de Academia Oamenilor de Știință din România, Nr. 2, 2015.
13. Jeff Crume, Doug Lhotka, Carma Austin, *Security and Artificial Intelligence,* published on https://www.ibm.com/downloads/cas/ZQROXRBK.pdf.

[10] Col. (r.) prof. univ. dr. Gheorghe Boaru, *Securitatea cibernetică în Uniunea Europeană,* Revista Academiei de Științe ale Securității Naționale, Nr.2, 2017, p. 66.

14. https://www.sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2019.pdf.
15. https://cybersecuritytrends.ro/securitatea-cibernetica-prima-linie-de-aparare-in-fata-impactului-inteligentei-artificiale/.
16. https://www.enisa.europa.eu/.
17. https://www.argility.com/argility-ecosystem-solutions/iot/machine-learning-deep-learning/.
18. https://www.ibm.com/security/artificial-intelligence.

THE ROLE OF CYBER AND ELECTROMAGNETIC ACTIVITIES ELEMENT IN ELECTROMAGNETIC ENVIRONMENT

Marius COSTACHE
Master Student, "Carol I" National Defence University,
mcostache@mapn.ro

***Abstract**: CEMA synchronizes capabilities across domains and warfighting functions and maximizes complementary effects in and through cyberspace and the electromagnetic spectrum. Intelligence, signal, information operations, cyberspace, space, and fires operations are critical to planning, synchronizing, and executing cyberspace and electronic warfare operations.*

The CEMA element is responsible for planning, integrating, and synchronizing Cyberspace Operations, Electronic Warfare and Spectrum Management Operations to support the commander's mission and desired end state within cyberspace and the electromagnetic spectrum.

***Keywords**: CEMA, Cyberspace Operation, Electronic Warfare, electromagnetic spectrum, Spectrum Management Operations.*

Technology will be an important element in a future conflict and a key factor in the dynamics of military organizations in the coming years. Maintaining the technological advantage in the key areas, will allow future armed forces to gain victory with small structures as a number, but professional ones. But these key capability areas were never integrated, which led to their interoperability only accidentally.

Conceptual delimitations regarding the cyber electromagnetic activities (CEMA).

During the Warsaw Summit (2016), NATO "recognize cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea. This will improve NATO's ability to protect and conduct operations across these domains and maintain our freedom of action and decision, in all circumstances. It will support NATO's broader deterrence and defence: cyber defence will continue to be integrated into operational planning and Alliance operations and missions, and we will work together to contribute to their success"[1].

Also at the Warsaw Summit, the heads of states and allied governments pledged to act as a priority to strengthen the cyber defence of national networks and infrastructures, to strengthen their resilience and the ability to respond quickly and effectively to cyber attacks, including in the context of hybrid actions.

The recognition of cyber space as an operational area represented a legitimate step in supporting NATO Alliance's ability to respond to cyber threats to its main interests and collective security. The Alliance, however, has adopted a retention policy and acts in accordance with international law, which stipulates that Allies will not use national-sovereign offensive cyber capabilities in NATO operations except in compliance with international law, including for operations under Article V. The existing international law represents the main framework for state behavior in cyber space, including the use of offensive cyber capabilities.

At the recent NATO summit in Brussels in 2018, although the strategic, operational and technical progress in addressing cyber malware was remarked, Allied leaders warned that

[1] Warsaw Summit Communiqué, Warsaw, 8-9 July 2016 accessed February, 22 on https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

cyber threats to Alliance security are becoming more frequent, more complex, destructive and coercive. The ongoing challenges require NATO to permanently evaluate both the nature of cyber threats and their own ways of adapting and responding.

They agreed on how to integrate sovereign cyber capabilities, which were voluntarily to the other operational areas, in particular through the continuous integration of all these activities in the operational planning process. This is one of the basic requirements in the context of the functionality operationalization of the cyber space.

From another perspective, the requirement to integrate and coordinate *activities in cyber space* with *activities in electromagnetic space*, under the concept of cyber and electromagnetic activities (Cyber and Electromagnetic Activities/CEMA), is a recent doctrinal concern, which deserves serious consideration given that the specific activities in both areas can be relatively easily assimilated and have similar effects: "Offensive cyber operations (activities that project power to achieve military objectives in, or through, cyberspace), Defensive cyber operations (active and passive measures to preserve the ability to use cyberspace), Cyber Intelligence, surveillance and reconnaissance (intelligence, surveillance and reconnaissance activities in, and through, friendly, neutral and adversary cyberspace to build understanding), Cyber operational preparation of the environment (all activities conducted to prepare, and enable, cyber intelligence, surveillance and reconnaissance, defensive and offensive operations)"[2].

United States Vision

United States Department of Defence understood the importance of cyber space and electromagnetic spectrum for the armed forces, publishing for the first time, in 2014, Field Manual 3-38 "*Cyber Electromagnetic Activities*", which provides the necessary information for the armed forces to conduct CEMA to enable them to model the operational environment and conduct joint ground operations. This handbook provides sufficient guidance to commanders and subordinate staff to develop innovative approaches about taking, retaining and exploiting benefits across the entire operational environment.

FM 3-38 defines CEMA as "activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system. CEMA consist of cyberspace operations (CO), electronic warfare (EW), and spectrum management operations (Figure 1)"[3].

At its heart, CEMA are designed to posture the Army to address the increasing importance of cyberspace and the electromagnetic spectrum (EMS) and their role in unified land operations. CEMA are implemented via the integration and synchronization of cyberspace operations, electronic warfare, and spectrum management operations (SMO).

The Army needs to look at four major functional areas relating to CEMA: identifying threats; protecting data from the threat; protecting the network from disruption; and the informational and operational dominance the Army needs to achieve with electronic warfare, information warfare and cyber[4].

[2] Joint Doctrine Note 1/18, *Cyber and Electromagnetic Activities*, UK Ministry of Defence, February 2018.

[3] Field manual 3-38, *Cyberspace Electromagnetic Activities*, February 2014.

[4] *Army CEMA Teams Advance Information, Electronic and Cyber Warfare*, accessed February 26, 2020, on https://www.afcea.org/content/army-cema-teams-advance-information-electronic-and-cyber-warfare.

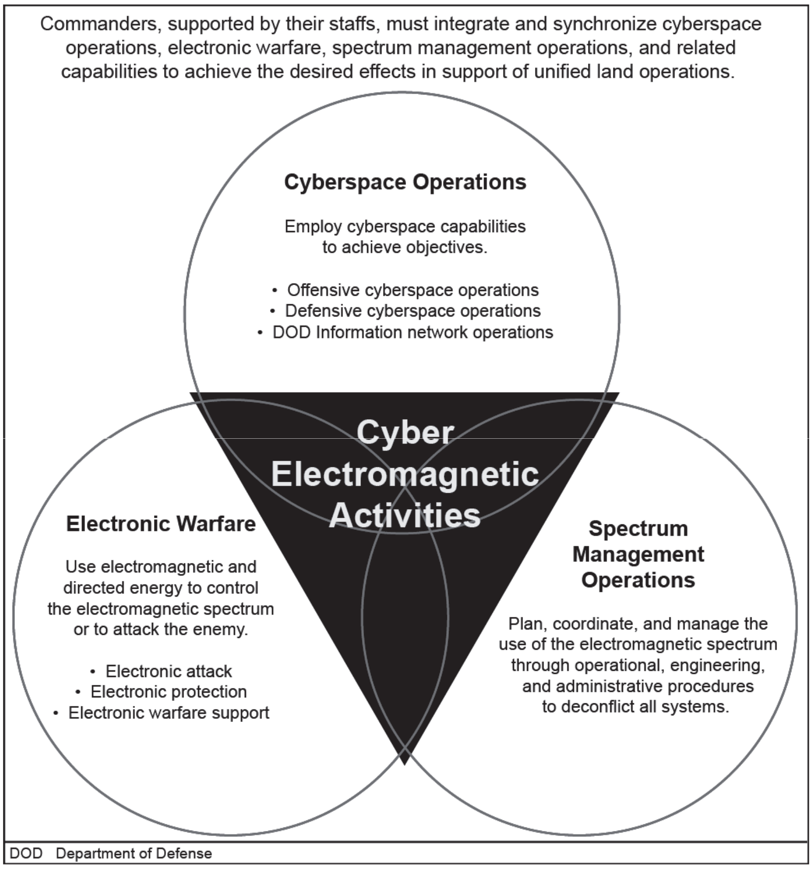

Commanders, supported by their staffs, must integrate and synchronize cyberspace operations, electronic warfare, spectrum management operations, and related capabilities to achieve the desired effects in support of unified land operations.
Cyberspace Operations
Employ cyberspace capabilities to achieve objectives.
• Offensive cyberspace operations
• Defensive cyberspace operations
• DOD Information network operations
Cyber Electromagnetic Activities
Electronic Warfare
Use electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.
• Electronic attack
• Electronic protection
• Electronic warfare support
Spectrum Management Operations
Plan, coordinate, and manage the use of the electromagnetic spectrum through operational, engineering, and administrative procedures to deconflict all systems.
DOD Department of Defense

Figure 1. Cyber electromagnetic activities[5]

CEMA integrates and synchronizes the functions and capabilities of CO, EW, and SMO to produce complementary and reinforcing effects. Conducting these activities independently may detract from their efficient employment. If uncoordinated, these activities may result in conflicts and mutual interference between them and with other entities that use the electromagnetic spectrum. CO, EW, and SMO are synchronized to cause specific effects at decisive points to support the overall operation.

The CEMA element is responsible for planning, integrating, and synchronizing CO, EW, and SMO to support the commander's mission and desired end state within cyberspace and the EMS. During execution the CEMA element is responsible for synchronizing CEMA to best facilitate mission accomplishment.

United Kingdom (UK) Vision

According to UK Joint Doctrine Note 1/18 CEMA vision is „*The synchronisation and coordination of cyber and electromagnetic activities, delivering operational advantage thereby enabling freedom of movement, and effects, whilst simultaneously, denying and degrading adversaries' use of the electromagnetic environment and cyberspace*"[6].

Recent efforts have concentrated on developing cyber forces and capability, and while significant progress has been made, development is often conducted along single-Service lines, except for offensive cyber. This is not a problem confined solely to the UK. Few North Atlantic Treaty Organization (NATO) members have developed a coherent and comprehensive cyber approach and NATO has yet to incorporate 'cyber' into its definitions and terms. While achieving consensus on the concept of CEMA is difficult, a debate may start

[5] Field manual 3-38, *Cyberspace Electromagnetic Activities*, February 2014.

[6] Joint Doctrine Note 1/18, *Cyber and Electromagnetic Activities*, UK Ministry of Defence, February 2018.

with the examination of the sub functions of core CEMA and how their scope interacts with each other; these being EMA and cyber activities, and their collective management.

Operationally there are four EMA that are key elements: electronic warfare; signals intelligence; spectrum management and communications. These functions are integral parts and interlinked in operations.

Roles, responsibilities and organization

CEMA element is composed of personnel who can plan, prepare and synchronize the actions of CO, EW and SMO. The CEMA element is led by the electronic warfare officer and provides the personnel all the necessary expertise to plan, integrate and synchronize CO, EW and SMO. On their turn, commanders organize their personnel based on mission requirements, strengths and weaknesses.

CEMA element integrates CEMA within the operational process from brigade level to corps level and is responsible for coordinating CEMA capabilities in supporting the operation conception. As part of the staff, CEMA element participates in the process of targeting and planning in order to be able to determine the desired effects in support of the operation concept.

CO, EW and SMO differ in terms of combat use and their tactics, but their functions and capabilities need to be integrated and synchronized to ensure that desired effects are produced. In the operational process, it must be considered that the CEMA element ensures the cyber space and the electromagnetic spectrum are used to the maximum to fulfill the general mission of the structure.

The CEMA element coordinates and synchronizes in the combat, both the offensive and the defensive elements of CEMA, being oriented towards the final state desired by the commander and developing, implementing the necessary actions to gain and maintain the freedom of action in the electromagnetic and cyber space.

Conducting cyber warfare and independent electronic warfare operations can lead to diminished efficiency. Conflicts, incidents and interference can cause the impossibility of communication, loss of intelligence or the degradation of the electronic protection capabilities of their own systems.

Starting with commanders, continuing with staff, assistant Chief of Staff, G-2, G-3, G-6, civil affairs operations G-9, fire support coordinator, IO officer, all of them are involved in plan, integrate and synchronize for cyberspace and EW.

I will present some of these activities, without pretending that I have included them all:

- "Plan, request, and synchronize effects in cyberspace and the EMS supporting freedom of maneuver.
- Coordinate with higher headquarters staff to integrate and synchronize information collection efforts to support cyberspace and EW operations.
- Synchronize cyberspace and EW effects requests with organic targeting capabilities.
- Prepare and submit effect requests using the CERF or electronic attack request format (EARF).
- Develop, maintain, and disseminate a common operational picture of designated cyberspace and
- EMS to enable situational understanding.
- Prepare for cyberspace and EW operations by conducting information collection activities, technical rehearsals, and pre-operation checks and inspections.

- Conduct SMO for the headquarters and subordinate units within the area of operations"[7].

Executing CEMA provides an advantage to maintain freedom of maneuver in cyberspace and the EMS. Coordinating and synchronizing the efforts of staff elements ensures available information is concentrated to make an appropriate decision based on impacts to current operations and the commanders' objectives.

Synchronizing cyber operations with electronic warfare ones, in the context of a complete spectrum approach, may exceed the capabilities of conventional forces that are not prepared for simultaneous action in the electromagnetic environment and cyber space.

The experience of recent conflicts, has shown us that the technological advantage has often been eroded using unconventional capabilities, using electromagnetic energy and cyber activities.

For this reason, armed forces must to continue to refine the CEMA concept for providing a more holistic approach to cyberspace operations and to insert these capabilities at lower levels in the order to accelerate decision-making and to provide cyber and electronic warfare options to the commander to get their objective. The Army CEMA concept seems to offer military staff an effective way of merging CO with those of EW and electromagnetic spectrum operations.

"*To succeed against complex and diverse threats that exploit the pervasive information environment we need to do things differently. At the heart of this concept is the enhancement of joint action and, therefore, our influence by contesting the information environment, being more integrated as a force and more adaptable to changing circumstances. Conventional and non-conventional adversaries may be state or non-state; and may employ mission-tailored, decentralized, asymmetric and agile actors. Therefore, it is important that we have doctrine that examines how we adapt operations to the changing environment rather than trying to control it*"[8].

BIBLIOGRAPHY

1. ****Field manual 3-38, Cyberspace Electromagnetic Activities, February 2014.*
2. ****Field manual 3-12, Cyberspace and Electronic Warfare Operations, April 2017.*
3. **** Joint Publication 3-12, Cyberspace Operations, June 2018.*
4. **** Joint Doctrine Note 1/18 Cyber and Electromagnetic Activities, February 2018.*
5. https://www.army.mil/article/198871/integrated_army_cyber_activities_teams_playing_pivotal_role_in_warfare
6. https://www.fifthdomain.com/dod/army/2018/07/05/how-the-army-will-infuse-cyber-operations-on-the-battlefield/
7. https://www.afcea.org/content/army-cema-teams-advance-information-electronic-and-cyber-warfare
8. https://www.army.mil/article/229083/why_the_cema_conference_brings_together_cyber_ew_and_sigint_on_ccdc_in_the_lab_podcast
9. https://fortgordonalliance.com/latestnews/integrated-army-cyber-activities-teams-playing-pivotal-role-in-warfare/
10. https://www.c4isrnet.com/electronic-warfare/2018/06/20/how-the-army-will-plan-cyber-and-electronic-warfare-operations/
11. https://monitorulapararii.ro/nato-fata-in-fata-cu-amenintarea-cibernetica-19-minute-pentru-a-reactiona-1-12560

[7] Field manual 3-12, *Cyberspace and Electronic Warfare Operations*, Department of the Army, April 2017.

[8] Joint Doctrine Note 1/18, *Cyber and Electromagnetic Activities*, UK Ministry of Defence, February 2018.

UNMANNED SYSTEMS IN COMBAT TYPE MISSIONS

Eduard Grigore JELER
LTC., PhD candidate, Military Technical Academy "Ferdinand I",
eduard_jeler@yahoo.com

Abstract: *Unmanned systems quickly transform the way of wars evolution all over the world - even if they are high technology stealth drones operated by the U.S. Army or a cheap commercial quadcopter modified by rebels from Syria for carrying their improvised bombs. In the next decade the intensive use of autonomous systems will be a standard practice in military operations. This fact is confirmed by the extensive use of unmanned aerial vehicles in Afghanistan, Iraq, Libya and Syria. In this article, we will take a quick look over the principal types of unmanned systems and the possible missions that they can perform, especially on UAV systems.*

Keywords: *US, UAV, UGV, USV.*

Introduction

The unmanned systems of weapons and military robots evolve from fiction films to the drawing boards of designers, to engineering laboratories and to the battlefield. In the current conflicts, one of the fastest growths of adopting innovative technology involves pilotless systems. The use of these systems by fighters not only changes the face of modern warfare, but also changes the decision-making process in combat operations. These systems are evolving rapidly to provide increased fighter capacity in multi-domain combat space[1]. The current combat operations continue to highlight the value of unmanned systems in the modern combat environment. Fighters appreciate the inherent characteristics of pilotless systems, especially persistence, versatility and reduced risk for loss of human life. The autonomous systems of these systems have a rapid growth in all areas: air, air and maritime. Systems without equipment offer various capabilities to perform operations across the entire range of military operations: surveillance and data collection; chemical, biological, radiological and nuclear (CBRN) detection; capabilities against improvised explosive devices (FDI); security of military bases. Moreover, the capabilities offered by these pilotless systems continue to expand. One factor contributing to the development of autonomous systems, especially small ones, is their relatively low production and operating costs. The cost of production is 25-40% lower than that of the equipped vehicles, while their operating cost is almost 80% lower. In addition to these advantages there is mobility, a possibility of rapid deployment in the theatre of operations, safe use, loss of personnel, simple training of operators. Another contributing factor is the progress in the creation of new building materials, light and economical engines, high-tech information communication platforms and navigation systems.

The advantages of using autonomous systems in combat can fall into two categories: military advantages and moral advantages.

1. Military advantages:

- Autonomous systems act as a force multiplier (fewer fighters are needed for a given mission, and each fighter's effectiveness is higher)
- Expanding the battlefield (allowing the fight to reach areas previously inaccessible).
- Smaller number of casualties (eliminating human warriors from dangerous missions) [2].

[1] https://smallwarsjournal.com/jrnl/art/designing-unmanned-systems-for-military-use-harnessing-artificial-intelligence-to-provide - accesat la data de 22.10.2019.

[2] Gary E. Marchant et al., "International Governance of Autonomous Military Robots," Columbia Science and Technology Law Review 12 (June 2011): 272–76.

2. Moral benefits:

- The ability to act in a non-conservative manner, more precisely they do not need to protect themselves. Armed autonomous systems' primary purpose should not be self-preservation and they may be used in a self-sacrificing manner, if necessary and appropriate, without the reservation by a commanding officer. These situations can be avoided such as" first time someone draws and then asks".
- Robotic systems without a pilot can be designed as being emotionless but without cancelling their judgment or showing anger or frustration during ongoing events, dangerous feelings during the fight, which lead to criminal behavior.
- Correctly solving a problem that has arisen, where human personnel could make mistakes based on the information received and misinterpreted due to fatigue or stress.
- Autonomous systems can integrate more information from multiple sources much faster than a real-time human could do it, before responding with lethal force.
- In the case of mixed human teams - unmanned systems the latter have the ability independently and objectively monitoring the ethical behavior on the battlefield on both sides and reporting the observed offenses.[3]

Autonomous systems-specific combat missions

In the combat zones the autonomous systems can carry out a series of missions, listed below but the list is not closed would be:

1. Recognition and surveillance: although the main mission for unmanned systems remains video surveillance, there is a growing demand for wide area search and multi-intelligence capability. Processing, exploitation and dissemination remain key areas that highlight the need for interoperability. Possible missions of this type are:

- The ability to find high-yielding nuclear CBRN materials or hazards and examine affected areas, while reducing staff exposure to these agents.
- The ability to discover IOD devices, as they are the main cause of victims in the current theatres of operations. Improving the military's ability to find, mark, and destroy explosive hazards and landmines is a significant effort.

2. Security: unmanned systems security operations by providing information on the threat and possibilities of direct engagement with fire.

3. Command, control and communications support: unmanned systems offer commanders the ability to expand an austere communications network regardless of environment and relief, thus improving effective command and control. Autonomous payload relay communication systems for network extension enable continuous network connectivity between network weapon systems, sensors, soldiers, leaders, platforms and command posts at all levels; in all phases of combat, while traveling on complex / urban terrain and in all weather conditions.

4. Fighting assistance. Unmanned systems are ideal for supporting a wide variety of combat support missions, including military information, military police, mission-specific for mine experts/ dynamiters and CRBN operations, "friend-foe-combatant-non-combatant" identification capabilities.[4]

The figure below shows the possibilities of using autonomous systems in combat missions.

[3] https://smartech.gatech.edu/bitstream/handle/1853/36516/Arkin_ethical_autonomous_systems_final.pdf - accesat la data de 19.12.2019 - accesat la data de 19.12.2019.

[4] Eyes of the Army U.S. Army Roadmap for UAS 2010-2035.

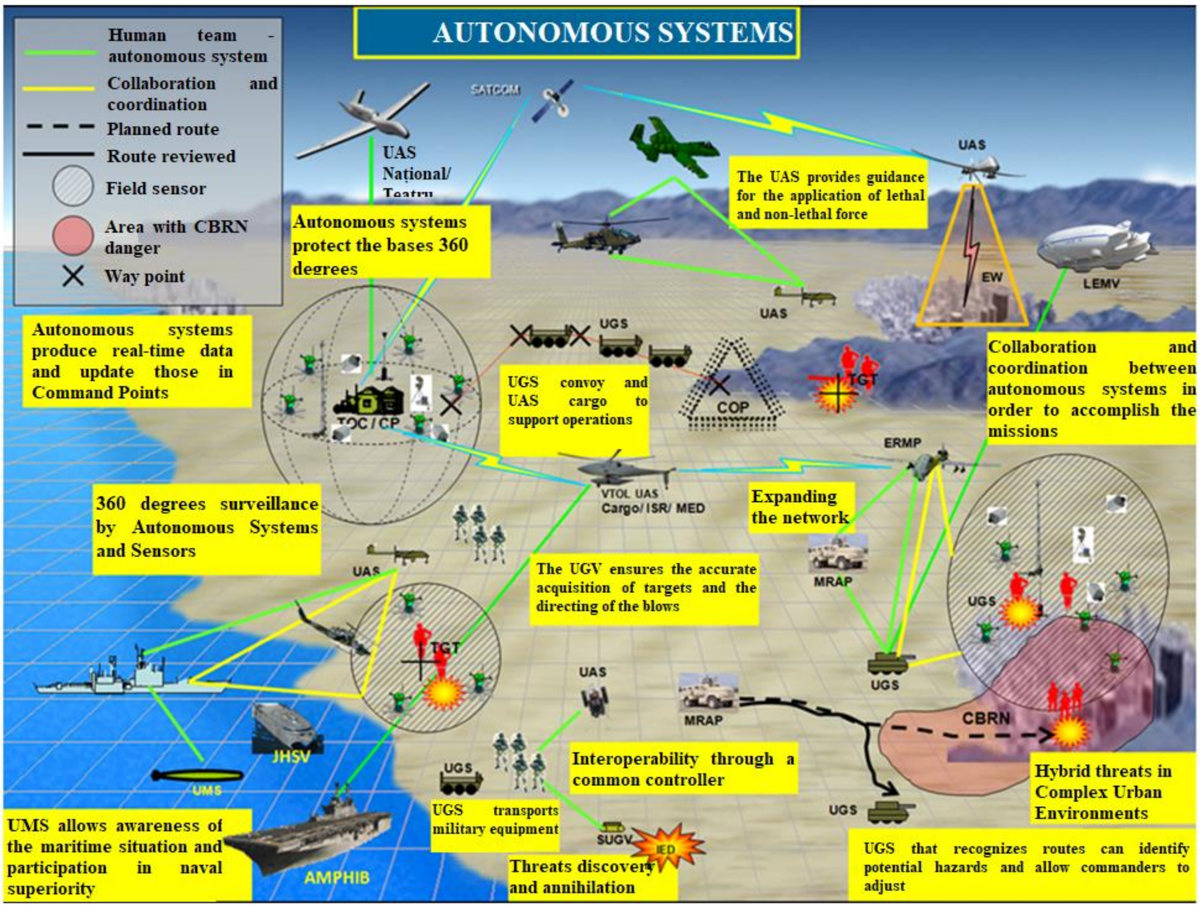

AUTONOMOUS SYSTEMS
Human team - autonomous system
Collaboration and coordination
Planned route
Route reviewed
Field sensor
Area with CBRN danger
Way point
SATCOM
UAS Național/ Teatru
Autonomous systems protect the bases 360 degrees
The UAS provides guidance for the application of lethal and non-lethal force
UAS
EW
LEMV
UAS
UGS
Autonomous systems produce real-time data and update those in Command Points
TOC/CP
UGS convoy and UAS cargo to support operations
COP
TGT
Collaboration and coordination between autonomous systems in order to accomplish the missions
ERMP
VTOL UAS Cargo/ ISR/ MED
Expanding the network
360 degrees surveillance by Autonomous Systems and Sensors
UAS
The UGV ensures the accurate acquisition of targets and the directing of the blows
MRAP
UGS
TGT
UGS
UAS
MRAP
CBRN
JHSV
UMS
Interoperability through a common controller
Hybrid threats in Complex Urban Environments
UGS
UGS transports military equipment
SUGV
IED
UMS allows awareness of the maritime situation and participation in naval superiority
AMPHIB
Threats discovery and annihilation
UGS that recognizes routes can identify potential hazards and allow commanders to adjust

Figura 1: The capabilities to use of unmanned systems in combat missions[5]

Examples of autonomous systems used in combat missions

UGV (Unmanned Ground Vehicle) - Unmanned ground vehicle primarily used for hazardous missions such as mining and demining. The new rover-style UGVs can also be useful to help soldiers carry heavy equipment, weapons and even wounded soldiers in and out of combat areas or to carry out security and surveillance missions. There is a tendency to create autonomous robots that will partner with humans and work in teams to create new combat formations.

UGCV (Unmanned Ground Combat Vehicle) - Unmanned ground fighting vehicle designed primarily to engage enemy forces with weapons. Because it is much more difficult for a ground vehicle to maintain a communication link outside the friendly territory than the air drones, it takes longer for the UGCVs to enter the operational service.

Military experts believe that the rapid pace of development of the UGCV reduces the number of soldiers in a tactical brigade by a quarter in the coming years. The trend shows that in the near future there are quality changes for the organizational matrix, the technical equipment and the combat capabilities of the ground forces.

Russia has created the Uranus family of robotic means for ground forces. Uran-6 is used to clean mines. Uran-9 is a multi-role device Uran-9 is specially designed to deliver combined units for fighting, reconnaissance and counter terrorism, with remote recognition and fire support. Uranus-14 designed to extinguish fires in environments that are life-threatening and inaccessible.[6]

[5] Initial Capabilities DocumentforUnmanned Systems (Air, Ground, and Maritime) Validation, JROC Interest.

[6] https://www.armyrecognition.com/weapons_defence_industry_military_technology_uk/analysis_combat_ugvs_ unmanned_ground_vehicles_for_military_forces_part_1.html - accesat la data de 22.10.2019.

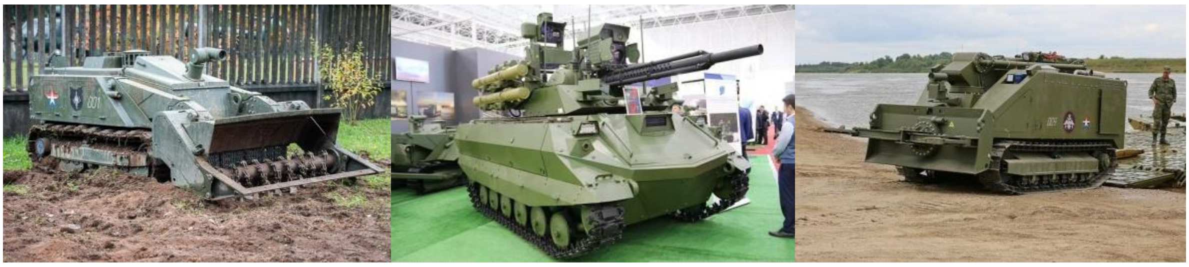


Figure 2: Autonomous systems in the Uran family (Uran 6, Uran 9, Uran 14) for ground forces[7]

USV (Unmanned Surface Vehicles): Unmanned Surface Vehicles, also known as unmanned surface vessels, are boats that operate on the surface of unmanned water. Pilotless marine vehicle systems are used in a variety of missions such as mine action, intelligence, surveillance and reconnaissance (ISR) services, anti-submarine warfare, and rapid attack craft.[8]

The RAFAEL company in Israel created the USV PROTECTOR made by it is an autonomous naval system capable of fulfilling a variety of naval and security missions. Originally designed for maritime security and force protection missions, PROTECTOR can also carry a new variety of modules that allow it to fulfill naval supremacy roles, such as precision blows and EW missions. Besides a series of sensors such as optics, the radar system can carry an automatic cannon, SPIKE missiles and a non-lethal water cannon.[9]

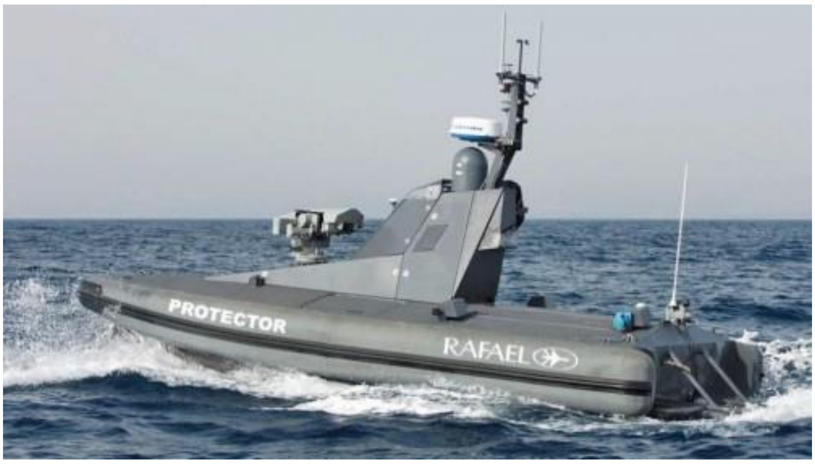


Figure 3: The autonomous naval system PROTECTOR USV made by RAFAEL[10]

UUV (Unmanned Underwater Vehicle): Underwater vehicle without pilot, are small systems used to retrieve objects from the seabed and even to carry out clandestine intelligence missions. search or submarine hunting and surface ships, driven by AI algorithms rather than human operators. In the future, Large Displacement Underwater Unmanned Vehicles (LDUUV) will appear, including autonomous underwater vehicles with high displacement

[7] https://www.armyrecognition.com/russia_russian_unmanned_aerial_ground_systems_uk - accesat la data de 28.10.2019.

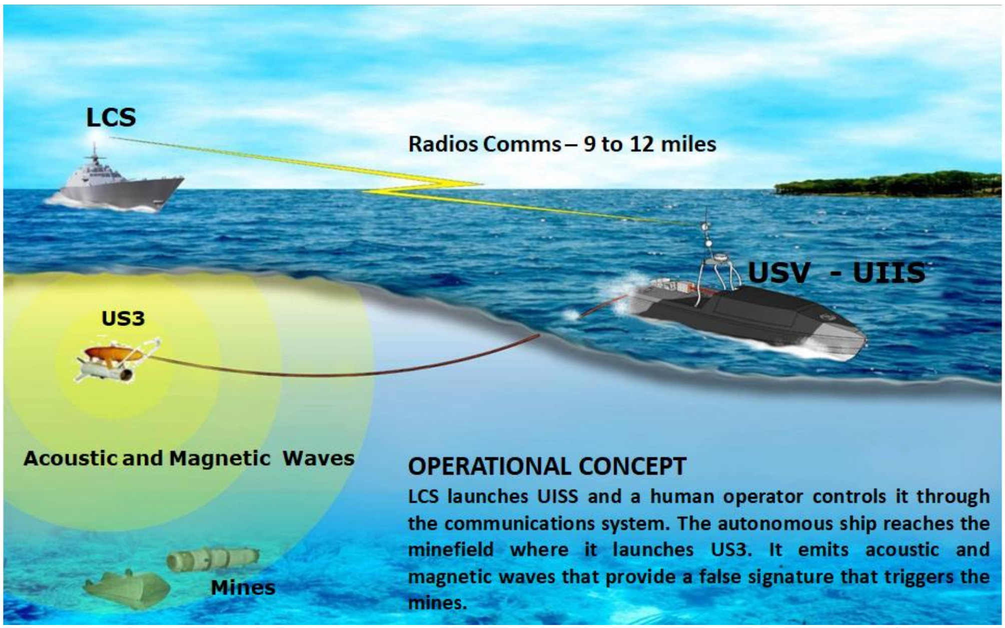
[8] Ru-jianYan, et all. Development and missions of unmanned surface vehicle, Journal of Marine Science and Application, December 2010, Volume 9, Issue 4, p. 452.

[9] https://www.rafael.co.il/wp-content/uploads/2019/03/Protector.pdf - accesat la data de 12.11.2020.

[10] https://www.rumaniamilitary.ro/usvunmanned-surface-vessel-protector-spartan-scout-si-aswusv - accesat la data de 15.11.2019.

capabilities that approach the size and capabilities of a complete system - the size of the submarine attack.

The figure below presents a possibility to use UISS (Unmanned Influence Sweep System – Autonomous Demining Systems). It consists of an underwater system and uses a generator of acoustic signals and magnetics provides a false signature that triggers mines. The surface ship during operation will be far enough away not to be damaged by a detonating mine.[11]

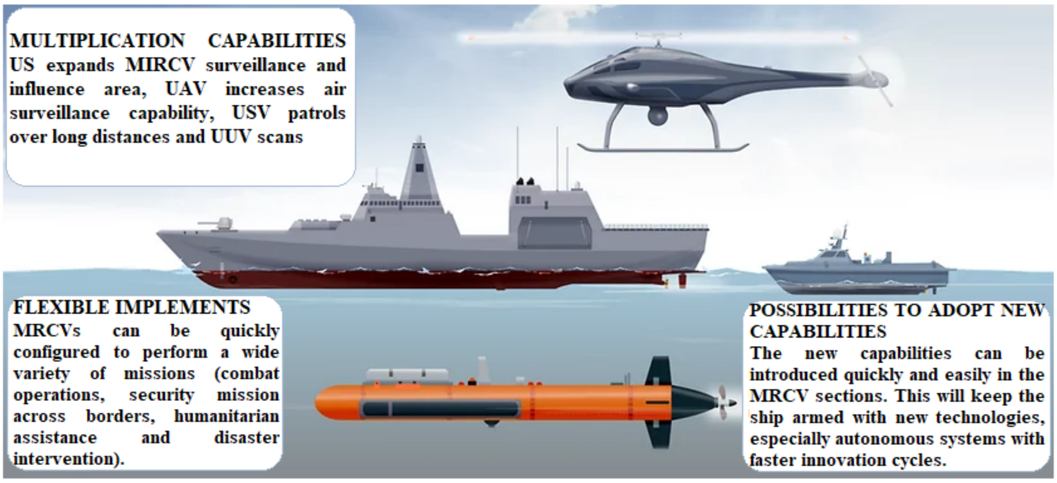


OPERATIONAL CONCEPT

LCS launches UISS and a human operator controls it through the communications system. The autonomous ship reaches the minefield where it launches US3. It emits acoustic and magnetic waves that provide a false signature that triggers the mines.

Figure 4: Use of the UISS system during a demining mission[12]

At the same time, the possibility of realizing the team of the ship with human crew - autonomous systems under the concept of MRCV (Multi-role Combat Ship - Multi-Role Combat Vessels), presented in the figure below, is being analyzed.



MULTIPLICATION CAPABILITIES

US expands MIRCV surveillance and influence area, UAV increases air surveillance capability, USV patrols over long distances and UUV scans

FLEXIBLE IMPLEMENTS

MRCVs can be quickly configured to perform a wide variety of missions (combat operations, security mission across borders, humanitarian assistance and disaster intervention).

POSSIBILITIES TO ADOPT NEW CAPABILITIES

The new capabilities can be introduced quickly and easily in the MRCV sections. This will keep the ship armed with new technologies, especially autonomous systems with faster innovation cycles.

Figure 2: Capabilities of MRCV system[13]

[11] https://www.militaryaerospace.com/unmanned/article/16722025/navy-moves-forward-with-unmanned-surface-vessel-with-embedded-computer-for-countermine-warfare - accesat la data de 22.11.2019.

[12] Duane Ashton, Unmanned Maritime Systems Overview, The Maritime Alliance Conference, 17 November 2010.

UAV (Unmanned Aerial Vehicle) An unmanned aerial vehicle, commonly known as a drone, is an unmanned aircraft. UAVs are a component of an unmanned aircraft system (UAS); which include a UAV, a ground controller and a communications system between the two. UAVs can operate with varying degrees of autonomy: either under remote control by a human operator or autonomous by on-board computers.[14]

The tasks assigned to the UAV vary depending on the technical and classification capabilities. Their most important missions are air reconnaissance, neutralization of air defence and electronic countermeasures, functioning as a communications relay, target designation, fire correction and damage assessment to the enemy and attack missions.

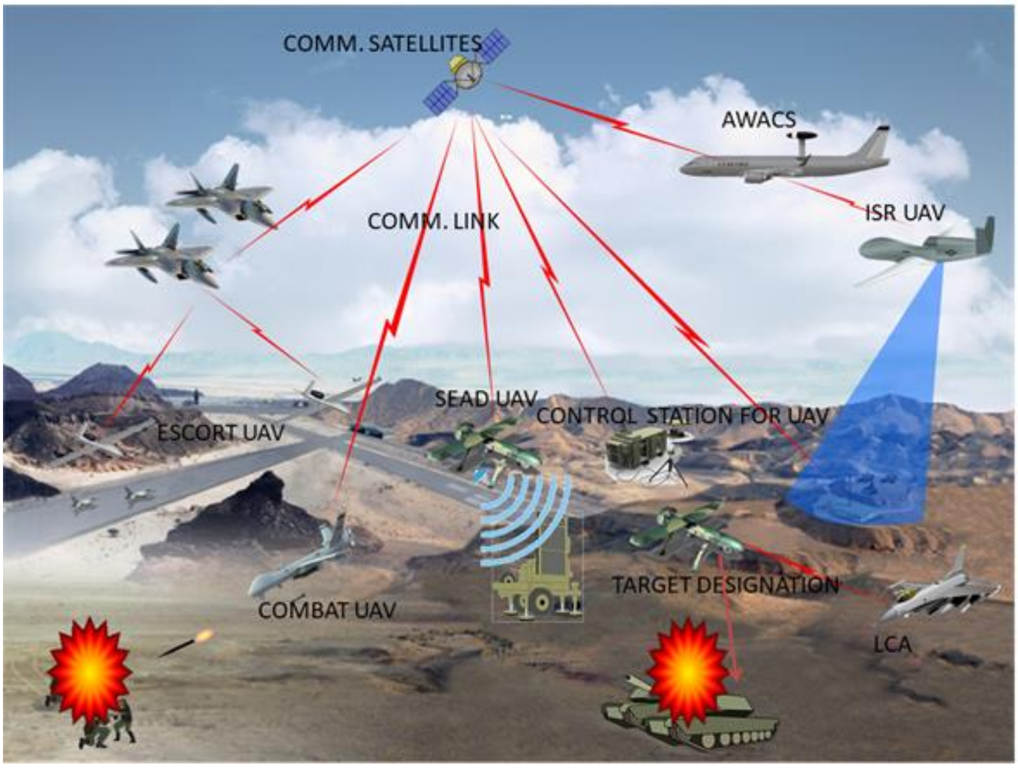


Figure 3: Use of UAS in the battlefield

UCAV (Unmanned Combat Aerial Vehicle) is an unmanned aerial system that has payload rockets or bombs being used in drone attacks. The most popular UCAV is MQ-9 Reaper, a remote piloted aircraft built by General Atomics, mainly used by USAF and CIA. Originally designed in the early 1990s for aerial reconnaissance and forward observation roles, has been modified and upgraded to carry and fire two AGM-114 Hellfire missiles or other types of ammunition[15].

[13] https://www.channelnewsasia.com/news/singapore/mothership-navy-submarine-hunter-recon-leader-unmanned-systems-11542998 - accesat la data de 29.11.2019.

[14] https://www.britannica.com/technology/unmanned-aerial-vehicle - accesat la data de 10.12.2019.

[15] https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104470/mq-9-reaper/ accesat la data de 12.12.2019.

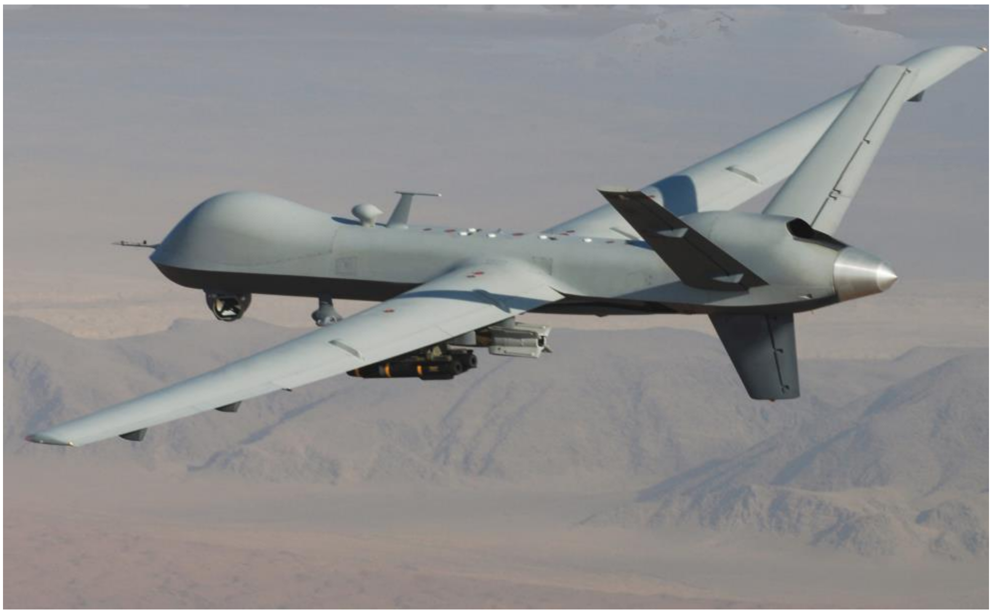
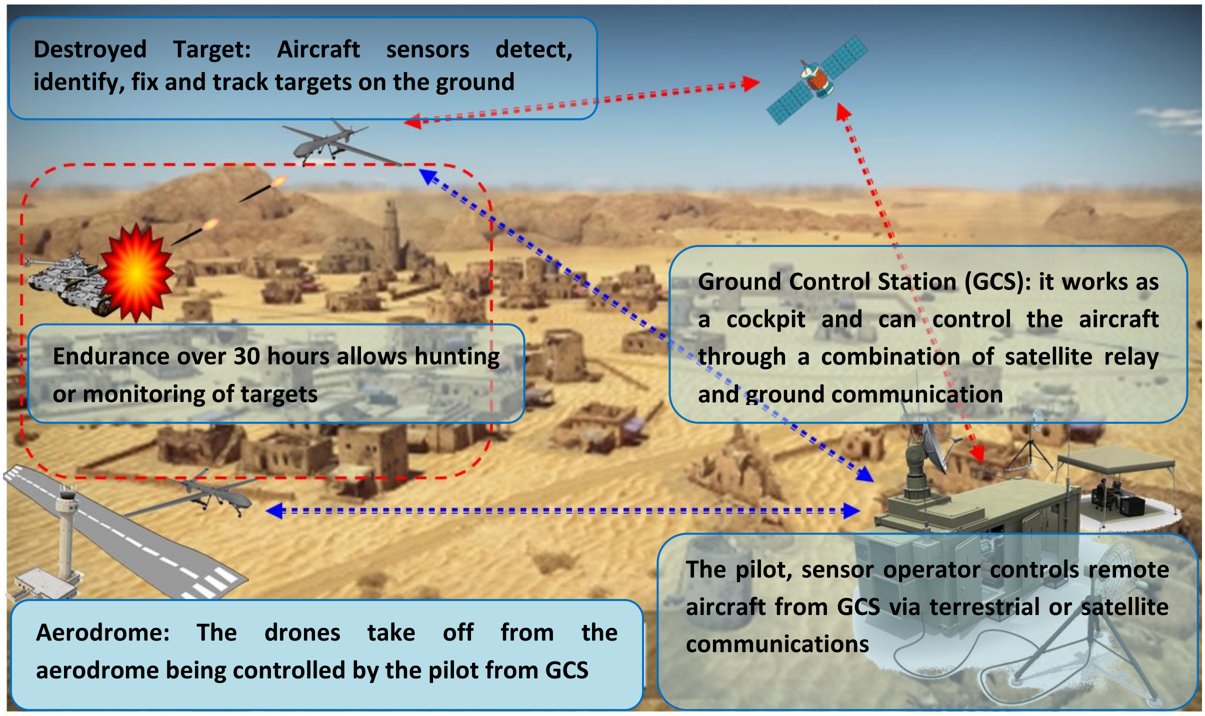


Figure 7: UAV MQ-9 REAPER system equipped with Hellfire rockets made by General Atomics Aeronautical[16]

The figure below shows how to use a UAS for air strikes. A typical system consists of several aerial vehicles, ground control stations, communications equipment and related personnel.



Destroyed Target: Aircraft sensors detect, identify, fix and track targets on the ground
Endurance over 30 hours allows hunting or monitoring of targets
Ground Control Station (GCS): it works as a cockpit and can control the aircraft through a combination of satellite relay and ground communication
The pilot, sensor operator controls remote aircraft from GCS via terrestrial or satellite communications
Aerodrome: The drones take off from the aerodrome being controlled by the pilot from GCS

Figure 8: Mission concept for using a UAV for an air strike[17]

[16] www.ga-asi.com – accesat la data de 16.12.2019.

[17] https://www.ibtimes.co.uk/raf-reaper-drone-strike-saves-isis-prisoners-public-execution-syria-1622038 - accesat la data de 22.12.2019.

Conclusions

- Autonomous systems have the following advantages: increasing situational awareness; easing the physical and cognitive tasks of the fighters; increased strength, efficiency and efficiency multiplier; facilitates movement and maneuver, reducing the number of casualties among the military.

- Problems that may arise are of a moral nature, the most obvious manifestation of this concern concerns the autonomous systems that are able to choose their own targets (probability of occurrence of unacceptable civilian collateral victims) and the problem of accountability according to the norms of international law humanitarian (the impossibility of identifying responsibility).

BIBLIOGRAPHY

1. *** Unmanned Systems Integrated Roadmap FY2011-2036.
2. *** Digital Infantry Battlefield Solution, Introduction To Ground Robotics, DIBS project Part I, December 2016.
3. Michael Franklin, Unmanned Combat Air Vehicles: Opportunities For The Guided Weapons Industry**,** Military Sciences Department, Royal United Services Institute for Defence and Security Studies, September 2008.
4. George Woodhams, John Borrie, Armed UAVs in conflict escalation and inter-State crisis**,** UNIDIR 2018.

INDEX OF AUTHORS

The publications consists of 252 pages.

”Carol I” National Defence University Typography
Bucharest/Romania, sector 5, 68-72 Panduri Street
e-mail: editura@unap.ro
Phone: 00-40-021-319.48.80/0215; 0453

441/18.03.2020 C. 117/2020