“CAROL I” NATIONAL DEFENCE UNIVERSITY
CENTRE FOR DEFENCE AND SECURITY STRATEGIC STUDIES

STRATEGIC IMPACT

No. 2 [91]/2024

Open-access academic quarterly, nationally acknowledged
by CNATDCU, indexed in CEEOL, EBSCO, Index Copernicus,
ProQuest, WorldCat and ROAD international databases

“CAROL I” NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE
BUCHAREST, ROMANIA

CONTACT ADDRESS
Șos. Panduri, no. 68-72, Sector 5, 050662, Bucharest, Romania
Phone: +4021.319.56.49; Fax: +4021.319.57.80
Website: https://cssas.unap.ro/index_en.htm
E-mail: impactstrategic@unap.ro

ISSN 1841-5784; ISSN-L 1841-5784; e-ISSN 1842-9904

CONTENTS

EDITOR'S NOTE

The second issue of 2024, volume number 91, comprises a collection of eight articles which deal with timely research findings within the realm of defence and security concepts, NATO and EU: policies, strategies and actions, trends and perspectives in geopolitics and geostrategy, intelligence studies, and aspects concerning emerging technologies. The edition continues with an interview with Vice Amiral Mihai Panait, PhD, Chief of the Romanian Naval Forces, followed by the *Book Review*, *Scientific Event* and *Guide for authors* rubrics.

The first rubric, ***Defence and Security Concepts***, brings to our readers' attention an article written by our colleague, Mrs. **Alexandra Sarcinschi**, PhD, Senior Researcher, which explores the importance of incorporating risk perception assessment into evaluating the impact of climate change on national security's societal dimension with the aim of creating a framework to guide future strategies and policies. The analysis emphasizes that climate change is just one factor contributing to a broader "permacrisis" which increases public stress and anxiety, and, based on existing surveys, the author draws some conclusions that outline key components for a framework to analyse climate change-related risks.

The second article, signed by Lieutenant-colonel **George-Ion Toroi**, PhD, highlights the role of deception in military operations, using the 2022 Kharkiv counteroffensive as a case study. By providing a detailed analysis of the strategies used, the author stresses the effectiveness of deception in modern warfare and extracts key lessons for future military planning, while also presenting the theoretical aspects of military deception and its influence on the outcome of the Kharkiv campaign, confirming enduring principles and methods used in the operation.

The heading ***NATO and EU: Policies, Strategies, Actions***, encompasses two articles: first, signed by Mrs. **Ilinca-Smaranda Cioată**, analyses Euro-Atlantic relations, pointing out that although cooperation between Europe and the United States is in question, a short-term political, military or economic rupture would have serious consequences at the global level; in the long term, the EU could become more militarily independent, but not completely. The paper focuses on the relationship between the EU and NATO, using the recent strategic documents of 2022 (EU Strategic Compass and NATO Strategic Concept) and the 2023 Joint Declaration, which reflect joint responses to new challenges. The objective is to emphasize the transatlantic partnership as an essential element of stability through common security and defence strategies.

The second paper under this rubric is written by Mrs. **Andreea Dincă**, and examines the EU-Africa partnership in the field of peace and security, highlighting EU's active role as a supporter and funder of African initiatives at national, regional and continental levels. Even though current discussions place this partnership in the context of global power competition, the article examines the explanatory role of the concept of strategic culture in this field, assessing events and trends after 2022 to determine whether EU actions in Africa reflect a coherent strategic culture. The paper concludes this approach helps to understand the EU's preferences, constraints and effectiveness in its security behaviour in Africa.

In the third rubric, ***Geopolitcs and Geostrategy: Trends and Perspectives***, the article written by Captain (N) Professor **Lucian-Valeriu Scipanov**, PhD, in co-authorate with Lieutenant (N) Junior Grade, Engineer, **Marian-Vasile Sava**, examines the complex environment of the seabed to highlight the importance of its control in maritime security. The authors explore the concept of "warfare on the bottom of the sea" and propose directions for the development of a specific doctrine or as part of a broader naval doctrine. The novelty of the article consists in the identification of the necessary directions for the control of the seabed and the possibility of integrating this concept into the doctrine of the Romanian Naval Forces.

Starting with this edition, we have included a new rubric in the journal, namely the ***Emerging Technologies***, which comprises two articles. The first, signed by Captain **Ionela Cătălina Manolache**, deals with the need for precise and adaptive protection measures in the current security environment, with a focus on safeguarding the transatlantic area, while highlighting the role of emerging and disruptive technologies in achieving this goal. Through documentary analysis, the paper explores how military leaders plan for the rapid movement of forces to potential conflict zones, emphasizing the importance of force protection and the integration of advanced technologies in meeting these efforts.

The second article, written by Colonel Engineer **Petru-Eduart Dodu**, PhD, stresses the growing impact of drones on various aspects of life. What once seemed unimaginable is now reality, with drones playing a crucial role in conducting atmospheric research, monitoring pollution and hazardous zones, improving domestic infrastructure surveillance, and enhancing military reconnaissance, leading to easier victories in conflicts. Conclusions lead to the fact that drone development continues, promising even greater advancements in the future.

In the ***Intelligence Studies*** rubric, we have included an article signed by Mr. **Cristian Condruț,** that emphasizes the increasing interest in cybersecurity education among public and private institutions, reflected in the availability of various academic and training programs. As cyberintelligence emerges as a critical subfield of both intelligence and national security, there is a pressing need for education and training

to develop analysts capable of addressing cybersecurity threats. The findings of the research indicate that high-priority competencies blend both intelligence and cybersecurity skills, with analytical and context-dependent abilities being the most significant. The paper also provides examples of educational practices that can be implemented to enhance these critical competencies.

Within the ***Strategic Dialogue*** rubric, we had the honour to interview Vice Admiral **Mihai Panait**, PhD, the Chief of the Romanian Naval Forces, on the security situation in the Black Sea in these challenging times.

Through the ***Book Review*** rubric, we want to bring to the readers' attention *Security Perception and Security Policy in Central Europe, 1989-2019*, a book edited by Mr. Tamas Csiki Vargha, and reviewed by our colleague, **Mihai Zodian**, PhD, Researcher.

The ***Scientific Event*** rubric briefly presents aspects from International Seminar "Lessons Identified from the Conflict in Ukraine", held by CDSSS on May 16th, 2024, in a hybrid format.

Also, this edition includes the ***Guide for authors***, a mandatory reading for those who wish to disseminate the research results in our journal.

For those discovering *Strategic Impact* for the first time, the publication is an open-access peer reviewed journal, edited by the Centre for Defence and Security Strategic Studies and published with the support of "Carol I" National Defence University Publishing House, and, also, a prestigious scientific journal in the field of military sciences, information and public order, according to the National Council for the Accreditation of University Titles, Diplomas and Certificates (CNATDCU).

Strategic Impact is an academic publication in the field of strategic defence and security studies. The journal has been published since 2000 in Romanian, and since 2005 in English, print and online. The journal is currently published exclusively in English. The articles are checked for plagiarism and scientifically evaluated (double blind peer review method). The thematic areas include political science, international relations, geopolitics, the political-military sphere, international organizations – with a focus on NATO and the EU information society, cyber security, intelligence studies, military history, and emerging technologies. Readers will find in the pages of the publication strategic-level analyses, syntheses and evaluations, views that explore the impact of national, regional and global dynamics.

In terms of international visibility − the primary objective of the publication − the recognition of the scientific quality of the journal is confirmed by its indexing in the international databases CEEOL (Central and Eastern European Online Library, Germany), EBSCO (USA), Index Copernicus (Poland), ProQuest (USA), and WorldCat and ROAD ISSN, as well as its presence in the virtual catalogues of the libraries of prestigious institutions abroad, such as NATO and military universities in Bulgaria, Poland, Czech Republic, Hungary, Estonia etc.

The journal is distributed free of charge in main institutions in the field of security and defence, in the academia and abroad − in Europe, Asia and America.

In the end, we encourage those interested in publishing in our journal to rigorously survey and assess the dynamics of the security environment and, at the same time, we invite students, master students and doctoral candidates to submit articles for publication in the monthly supplement of the journal, *Strategic Colloquium*, available at URL: http://cssas.unap.ro/ro/cs.htm, indexed in the international database CEEOL, Google scholar and ROAD ISSN.

Editor-in-Chief, Colonel Florian CÎRCIUMARU, PhD
Director of the Centre for Defence and Security Strategic Studies

DOI: 10.53477/1842-9904-24-6

PERMACRISIS, CLIMATE CHANGE AND SOCIETY. TOWARDS A FRAMEWORK FOR ANALYSIS: RISK PERCEPTION COMPONENT

*Alexandra SARCINSCHI, PhD**

The paper discusses the relevance of incorporating risk perception assessment into the analysis of the impact of climate change on the societal dimension of national security. The objective is to develop a framework for analysis that will provide a coherent basis for future strategies and policies in this area. In order to address this issue, it is first necessary to acknowledge that climate change is just one of a number of phenomena and events contributing to the global permacrisis that causes stress and anxiety to the population. The second section of the paper presents a review of the relevant literature. Our aim is to determine whether it is appropriate to assess the risk perception in this context. Having conducted an assessment based on existing surveys, we will then draw conclusions on the essential elements of a framework for analysing climate change-related risks.

Keywords: *climate change; permacrisis; risk; risk perception; vulnerability; hazard; exposure*

The international agenda is currently focused on a number of issues that have the potential to shape the future of humankind. From one perspective, we are confronted with a multitude of global issues, including climate change, pandemics and the economic crisis. These in themselves could be regarded as threats to national and international security. Additionally, there are tendencies that originate from the aspiration of state and non-state actors to exert their influence on the international stage. These include competition for power and conflict, strategic competition in the outer space, and, last but not least, the hybrid actions of certain states.

**** Alexandra SARCINSCHI, PhD, is Senior Researcher within the Center for Defence and Security Strategic Studies, "Carol I" National Defence University, Bucharest, Romania. E-mail: sarcinschi.alexandra@unap.ro***

Climate change is a phenomenon that affects all countries, regardless of their geographical location, level of development, or status on the international stage. The way in which people represent the associated risks is a defining factor in shaping responses to this threat. In this context, the objective of the project entitled "The Impact of Climate Change on Romania's National Security"[1] is to construct a framework for analysing the aforementioned impact. The purpose of this paper is to discuss the fundamental elements of the analysis of the societal dimension, with a particular focus on the psychosocial aspects.

It is important to note that the perception of risk associated with climate change is not independent from the perception of risk in other areas of social life. A failure to consider the numerous factors that may impact security when measuring climate change would render the methodology employed. Indeed, climate change is itself influenced by and influencing a number of other factors, including societal, economic, military and political ones.

The scientific validity of this approach is supported by a literature review of the methodological frameworks employed in the field, as well as by reference to scientific studies conducted by institutions engaged in the investigation of risk perception in relation to climate change. Thus, in what follows, we will first discuss the relation between the crises affecting humankind, implicitly assuming that climate change is a particularly important element of the global permacrisis. In the second part of the paper, we discuss the role of risk perception in a potential framework for analysing the impact of climate change on the societal dimension of security. Finally, we compare risk perceptions longitudinally (in time) and cross-sectionally (between countries and regions) in order to underline the peculiar characteristics of climate change (it evolves in time and its impact differs from region to region) and to understand the social dynamics associated with this challenge.

1. Does Climate Change Constitute an Element of Global Permacrisis?

In the preceding five years, the overall context has become increasingly complex.

The consequences of the COVID-19 pandemic have been predominantly observed in economic and social area. Consequently, one of Europe's most significant challenges, namely mixed migration, has been less prominent in the public discourse, as national governments have implemented measures to address the health crisis, restrictions on international travel included. Nevertheless, this has not precluded

[1] ***Disclaimer**: This project is included in the "Sectoral Research & Development Plan of Ministry of National Defence for the period 2022-2025" and is developed in the period 2022-2024 by the Centre for Defence and Security Strategic Studies of the "Carol I" National Defence University at the request of the Armament General Directorate.*

the potential for a deterioration of the humanitarian situation in refugee camps or an increase in population movement to European countries as restrictions are lifted. The year 2023 registered the highest level of migration to Europe since the 2015-2016 crisis. Concurrently, the so-called "COVID-19 recession" (Cardani, et al. 2023) has resulted in the intensification of disparities between social groups, on the one hand, and between countries at different levels of development, on the other.

The war in Ukraine has triggered a significant influx of refugees into neighbouring countries and the rest of Europe. Similarly, the ongoing conflict in the Gaza Strip has led to the displacement of over 80% of the population. Furthermore, the political and military crises and conflicts that have emerged or intensified in Africa and the Middle East over the past two years have contributed to an exacerbation of the humanitarian crisis in regions that are already characterised by high levels of poverty.

The pre-war economic crisis was coupled with changing demand in the labour market and the economic outlook after the COVID-19 pandemic had a negative impact on societies and led to a new migration flow. In addition, climate change and related events are causing, now and in the future, not only internal displacement of populations affected by natural disasters (Türkiye, Syria, Afghanistan, Morocco, etc.), but also international migration from areas most vulnerable to the effects of global warming (Africa and Latin America) to developed countries.

We are therefore discussing a considerable number of disruptive events that have been occurring over an extended period of time. In addition to the destructions and human and material losses, the effects and perception of insecurity caused by these events persist. It can be argued that humankind is currently experiencing a *permacrisis*, a period in which significant events and phenomena, including conflicts, crises, persecution, extreme poverty, human rights violations, and natural disasters, occur simultaneously or in succession.[2]

It can be observed that in this series of events and phenomena, climate change appears as a constant. It is defined in Article 1 of the *United Nations Framework Convention on Climate Change* and encompasses not only the factors that determine

[2] A detailed analysis of the events and phenomena presented in this section is provided by the author in the series „Evaluare strategică" (Strategic Evaluation) published by the Centre for Defence and Security Strategic Studies of the "Carol I" National Defence University: "Criza «uitată» a Europei: impactul pandemiei de Covid-19 asupra populației de refugiați și migranți ilegali", in *Evaluare strategică 2020. Securitatea, între pandemie și competiție*, "Carol I" NDU Publishing House, 2021, pp. 69-94; "Migrația internațională în 2021: de la instrumentalizare și securitizare la criză umanitară de durată", in *Evaluare strategică 2021. Coordonate ale insecurității*, "Carol I" NDU Publishing House, 2022, pp. 75-110; „«Permacriză» umanitară? Războiul din Ucraina, insecuritatea percepută și acutizarea crizei umanitare", in *Evaluare strategică 2022. Lumea între pandemie și război*, "Carol I" NDU Publishing House, 2023, pp. 164-207; "Intensificarea mișcărilor de populație ca efect al permacrizei globale", in *Evaluare strategică 2023. Riscuri, incertitudine, război*, "Carol I" NDU Publishing House, upcoming.

it, but also the temporal aspects of climate change: "a change of climate which is attributed directly or indirectly to human activity that alters the composition of the global atmosphere and which is in addition to natural climate variability observed over comparable time periods" (UN 1992). This definition was further elaborated by a UN agency, the Intergovernmental Panel on Climate Change (IPCC), and the temporal dimension became even more visible: "A change in the state of the climate that can be identified (e.g., by using statistical tests) by changes in the mean and/or the variability of its properties and *that persists for an extended period, typically decades or longer*" (IPCC n.d.).

According to the generally accepted definition, climate change represents obviously a defining element of the global permacrisis. It is therefore imperative to conduct a detailed analysis of its impact on national security in order to identify the most effective strategies for mitigating its consequences for human society.

2. Risks and Society – Theoretical Framework

The available literature and empirical evidence collectively demonstrate that climate change can act as an enabling agent, thereby generating risks in societies that are often already vulnerable. The same literature emphasises that society is not only the passive, referent object of security (which must be protected), but also a producer of security or insecurity, along with all state and non-state actors involved (The Hague Centre for Strategic Studies 2012).

An analysis of this matter should focus on concepts such as climate security, climate change-related risks, resilience, psychosocial representation, social acceptability of climate change, cognitive bias, and so forth. Nevertheless, as the approach is of a very broad nature, at this stage of the project we will restrict our discussion to the issue of risk and risk perception.

In recent years, the term *climate security* has gained increasing attention in academic and policy circles. The Centre for Climate and Security (Washington) proposes a comprehensive conceptual framework based on four interrelated elements: climate change (rising greenhouse gas emissions; rising global temperature; rising sea levels), natural hazards (climate-related events: floods, tropical storms, landslides, heat waves, droughts, forest wildfires), and human systems (risk factors: vulnerabilities such as a lack of adaptive capacity and resilience, as well as exposed elements and socio-economic and institutional sensitivity) (The Centre for Climate and Security 2021, 20). Additionally, there are the drivers of insecurity that affect climate change (adverse impacts: mortality and morbidity, environmental degradation, infrastructure and livelihoods, health problems, inequality, resource availability and quality, social tensions, migration and internal displacement, unstable institutions, etc.) (The Centre for Climate and Security 2021, 20).

The security or insecurity of an actor is contingent upon a number of factors, including the nature and severity of the threat to which they are exposed, as well as the characteristics of the actor themselves, such as their vulnerability and resilience to harmful events.

There are several models for analysing the perception of climate change risk. These range from purely positivist approaches to constructivist ones such as the Climate Change Risk Perception Model (CCRPM) developed by van der Linden (van der Linden 2014) (van der Linden 2015) (van der Linden 2017), to models that combine scientific knowledge with experiential processing, socio-cultural influences and trust in sources of information alongside socio-demographic factors, such as the CCRPM+ (van Eck, Mulder and van der Linden 2020).

One of the most commonly used models of analysis that includes both objective and subjective factors was originally proposed by the IPCC and later commented on by Australian Professor John Handmer, an expert in Risk and Resilience at the International Institute for Applied Systems Analysis.

In the case of the IPCC, the definition of risk has been subject to change depending on the membership of the working groups that were established for the purpose of assessing the impacts of climate change. The IPCC Glossary currently operates with the following definition: "the potential for adverse consequences for human or ecological systems, recognising the diversity of values and objectives associated with such systems. In the context of climate change, risks can arise from potential impacts of climate change as well as human responses to climate change. Relevant adverse consequences include those on lives, livelihoods, health and well-being, economic, social and cultural assets and investments, infrastructure, services (including ecosystem services), ecosystems and species" (van Diemen 2019). It should be noted that the IPCC employs the term "risk" exclusively in reference to the adverse consequences of climate change. In instances where both negative and positive effects are considered, the recommended terminology is "climate impact driver". The definition also encompasses potential consequences for physical, human, and ecological systems. Additionally, it is acknowledged that each individual or community will assess negative consequences to systems according to their cultural model (Reisinger, Howden and Vera 2020). Therefore, this definition includes an important societal dimension and especially a cultural component that, according to various authors, is focused on the previous experience with disasters and perception of risk (Prior, et al. 2017). There are authors who argue that this dimension focuses mainly on societal organization and collective aspects, while the individual is studied more when considering psychosocial trauma related to disaster (Cardona, et al. 2012).

In this framework, there are authors who consider the theory of social representation better suitable for understanding the cultural and social dimensions of risks related to climate change (Joffe 2003) (Machin Suarez 2021). They are

arguing the idea that studying risk perception, even if it claims to study a collective phenomenon, does not contain any other support than the statistical behaviour of these data and is valid only for making decisions on political, economic or social issues (Machin Suarez 2021, 116).

Indeed, social psychology, as represented by the Romanian Serge Moscovici, defines social representations as a system of values, notions, practices related to objects, aspects or dimensions of the social environment. These determine the field of possible communications, values or ideas existing in the shared visions of groups and regulate the allowed behaviours (Neculau 1996) (Seca 2008) (Markova 2004). Willem Doise further emphasizes their main characteristic, defining them as "shared realities" and "position-generating principles" (Doise and Palmonari 1996) (Neculau 1996), thus emphasizing the communication and reaction components. Furthermore, Gerar Duveen argues that representations, supported by the social influence of communication, constitute everyday realities and serve as the primary means of establishing the affiliations by which we are bound to one another (Duveen 2001, 2). Summarizing, W. Wagner, G. Duveen, R. Farr, S. Jovchelovitch, F. Lorenzi-Cioldi, I. Marková and D. Rose, define social representations as a set of thoughts and feelings expressed through the verbal and overt behaviour of actors that constitute an object for a social group (Wagner, et al. 1999, 96).

It can be concluded that both the analysis of risk perceptions and social representations are important in the context of climate change. Strategies and policies to manage the effects of climate change, whether positive or negative, are based on both quantitative and qualitative risk assessment and vulnerability analysis. In this process, subjectivity, uncertainty and even optimistic bias play an important role. It should be noted, however, that the analysis of risk perception has the advantage of employing less costly and more straightforward methods and techniques, whereas the analysis of social representations of risk necessitates the utilisation of more sophisticated methodologies (Lo Monaco, et al. 2017).

Returning to the IPCC model, another element characterized by a high degree of subjectivity is vulnerability. It is a key element in defining risk and is the result of the dynamic interactions between climate hazards, exposure and vulnerability of the affected human or ecological system to hazard (van Diemen 2019).

Hazard is defined as "The potential occurrence of a natural or human-induced physical event or trend that may cause loss of life, injury, or other health impacts, as well as damage and loss to property, infrastructure, livelihoods, service provision, ecosystems and environmental resources" (van Diemen 2019). In light of the fact that climate change is regarded as a threat by the most prominent agencies in this field, including the UN (Intergovernmental Panel on Climate Change) and the EU (European Environment Agency), it seems reasonable to suggest that the potential for harm posed by climate change could be considered a security threat in its own

right. However, within the context of Anglo-American intelligence literature, the notion of a threat being posed by a force of nature or climate change is not accepted. Consequently, when the threat originates from an "agent" that is not human, the term "hazard" is employed (Prunckun 2015, 284).

The exposure relates strictly to the presence of units that may be adversely affected: people, livelihoods, species or ecosystems, environmental functions, services, resources, infrastructure, economic, social, or cultural assets in places and settings (van Diemen 2019).

Vulnerability is defined as "The propensity or predisposition to be adversely affected. Vulnerability encompasses a variety of concepts and elements, including sensitivity or susceptibility to harm and lack of capacity to cope and adapt." (van Diemen 2019).

The discussion on vulnerability is more complex because vulnerability can be assessed using several methods. They can be quantitative, qualitative or combined and can be centred on the analysis of data on losses (resulting in a comprehensive picture of direct, indirect and intangible losses), of structural data (census or statistical analysis of past disasters, but do not capture the multidimensionality of vulnerability) or of perceptions of vulnerability (useful for understanding social dynamics, but costly and time-consuming) (Prior, et al. 2017).

Building on the foundations of this methodology, as well as the approaches employed by Emergency Management Australia and the Australian/New Zealand risk management standard, John Handmer puts forth an alternative framework that emphasises a proactive and constructive approach to vulnerability, viewing it as an inherent capacity for resilience in the face of change (Handmer 2003). It also emphasizes the limits of the hazard – exposure – vulnerability triangle, especially in the case of complex hazards that may have no clear spatial or temporal boundaries, and possibly no agreed solutions, such as zoonosis (Handmer 2003, 56). He suggests the term "complex unbounded risks" that are hard to quantify due to the lack of acknowledged history, largely invisible, resist definition in space and time, may be accompanied by a climate of fear and an increase of concern and anxiety over time. Also, in this context, the evolution of the situation is getting worse and the impacts may be irreversible and on large scale (Handmer 2003).

Still, strictly in the case of climate change, the triangle of risk suggested by IPCC recognises the uncertainty of both risks and hazards and the need for both quantitative and qualitative evaluation (Reisinger, Howden and Vera 2020).

It can be observed that Handmer's model also incorporates the concept of risk perception, albeit without the use of that specific term. This is evident in his reference to the climate of fear, concern, and anxiety that may increase over time (Handmer 2003, 56). This indicates that the model is concerned with the subjective judgments that individuals make regarding the characteristics and severity of a risk.

Therefore, one of the first steps in analysing the impact of climate change on national security, alongside objective aspects of previous events, should be the measurement of risk perception

3. Risk Perception

The issue of climate change is perceived by a large part of the world as a significant risk. The most comprehensive survey of its kind, the *People's Climate Vote 2024*, was published by the UNDP this year. It comprises a sample of more than 73,000 individuals from 77 countries. The main finding is that there is a growing concern about climate change, with 53% of those surveyed indicating that they are more worried than in the previous year, compared with 15% who stated that they are less worried (Flynn, et al. 2024, 24). Also, 43% consider that extreme weather events were worse than usually this year than the last (Flynn, et al. 2024, 37). In terms of the impact of climate change on their daily lives, 69% of respondents indicate that it is already influencing their major decisions (such as where to live, where to work, and what to purchase), particularly in less developed countries that are most vulnerable to climate change (e.g., Kenya, Afghanistan, Uganda, Niger, Madagascar, Haiti, etc.) (Flynn, et al. 2024, 33-36).

However, where does climate change rank in the plethora of crises mankind is facing in terms of perceived associated risk? An analysis in this respect also needs to be made in relation to the other main security issues covered by the permacrisis. Following a comprehensive review of the most significant reports on risk perception, we have identified four key areas of concern: war, terrorism, economic crises and pandemics. These will be compared with the perception of climate change-related risks. In order to achieve this, the most recently published data from recent reports that sample more than ten countries, both global and regional in nature, will be discussed: *Lose-Lose? Munich Security Report 2024*; *The Global Risks Report 2024. Insight Report* of the World Economic Forum, and *Special Eurobarometer 538. Climate Change* of the European Commission.

The Munich Security Report 2024 identifies a number of risks for analysis, concluding that environmental threats are of particular importance and that the perception of the risk of mass migration as a result of war or climate change is increasing (Bunde, Eisentraut and Schütte, et al. 2024, 2). The security index is a multidimensional assessment of perceived risks, encompassing five key dimensions: overall, trajectory, severity, imminence, and preparedness. This assessment is based on the responses of a representative sample of approximately 1,000 individuals from 11 countries, including members of the G7 and BICS (Brazil, China, India, and South Africa).

The analysis of "climate change generally" as a risk and stress factor in the G7 countries reveals a downward trend in the score. In February/March 2021, the

perceived risk was ranked fourth, while in November 2021 it was ranked first. It then fell to fifth place in the October/November 2022 survey and finally to sixth place in the October/November 2023 survey (Bunde, Eisentraut and Knapp, et al. 2022) (Bunde, Eisentraut and Schütte, et al. 2024). For the BICS countries, this risk is perceived as the most significant over the entire period under analysis, with "extreme weather and forest fires" and "the destruction of natural habitats" representing the next most important issues.

Related to climate change and deriving from it can be considered at least five more risks from the list analysed by the authors of the report: "extreme weather and forest fires", "destruction of natural habitats", "mass migration as a result of war or climate change", "food shortages", and "a future pandemic". The perception of risk with respect to each of these issues is subject to fluctuation. However, in the most recent report, the risk associated with "extreme weather and forest fires" was identified as the most significant, having remained within the top three perceived risks for the past three years. The following table illustrates the aforementioned statements. It should be noted that, for purposes of comparison, this analysis also includes other risks that, at the initial publication of the security index (February/March 2021), occupied higher positions on the risk bump chart.

Table no. 1: Aggregate ranking of selected risks, 2021-2023, according to various editions of the *Munich Security Index*
Source: (Bunde, Eisentraut and Knapp, et al. 2022)
(Bunde, Eisentraut and Schütte, et al. 2024)

Risks (selection)	Aggregate rankings of risks			
	February/March 2021*	November 2021	October/November 2022	October/November 2023
Extreme weather and forest fires	2 —	2 ↘	3 ↗	**1**
Cyberattacks on your country	7 ↗	4 ↘	7 ↗	**2**
Destruction of natural habitats	3 —	3 ↘	4 ↗	**3**
Russia	24 ↗	15 ↗	1 ↘	**4**
Radical Islamic terrorism	14 ↗	9 ↘	22 ↗	**5**
Climate change generally	4 ↗	1 ↘	5 ↘	**6**
Mass migration as a result of war or climate change	15 ↗	10 ↘	12 ↗	7
A future pandemic	5 ↘	6 ↘	18 ↘	**22**
Food shortage	20 ↘	21 ↗	18 ↘	**24**
The coronavirus pandemic	1 ↘	5 ↘	26 ↘	**30**

* In the February/March 2021 report, the aggregate ranking of risks targets the G7 and BRICS countries. In subsequent surveys, however, the score indicates the perception of risk in the G7 countries alone.

In contrast to the MSI, the World Economic Forum (WEF) employs a sample of nearly 1,500 experts in the field to assess global risk perceptions. Furthermore, it conducts network analysis of perceived risks, which the aforementioned report does not. The risk landscape is analysed over three-time horizons: the present (2023-2024), the next two years and the next ten years. In all three periods, environmental risks are identified as the most likely to present a material crisis on a global scale, according to the perception of those surveyed (World Economic Forum 2024, 7). In this category, the WEF introduces six issues, which can be considered either causes or consequences of climate change: "extreme weather events", "critical change to Earth systems", "biodiversity loss and ecosystem collapse", "natural resource shortages", "pollution", and "non-weather related natural disasters".

For 2023-2024 period, the most likely environmental risk to present a material crisis on a global scale is perceived to be "extreme weather events" by 66% of the responders. In short time (2 years), it drops on the 2nd place, after "misinformation and disinformation" (1st), and before "societal polarization" (3rd), "cyber insecurity" (4th) and "interstate armed conflict" (5th). By contrast, in the long-term forecast, the top four positions are occupied by environmental risks ("extreme weather events", "critical change to Earth systems", "biodiversity loss and ecosystem collapse", and "natural resources shortages") (World Economic Forum 2024, 11, 13). Table no. 2 illustrates the evolution of perceptions regarding the aforementioned risks and the risks with which they are in a state of influence.

In terms of correlating different categories of risks, the experts interviewed establish a direct influence relation between all five environmental risks and risks such as "involuntary migration" (high influence node), "chronic health conditions" (medium influence node), "infectious diseases" (medium influence node), and "economic downturn" (high influence node). Thus, "natural resource shortages", "critical change to Earth systems", "extreme weather events", "pollution", and "non-weather related natural disasters" are perceived as directly determining "involuntary migration" as a societal risk. Additionally, another societal risk, "infectious diseases" are regarded by experts as being driven by "critical change to Earth systems", "natural resource shortages", "pollution", "extreme weather events", "biodiversity loss and ecosystem collapse", and "non-weather related natural disasters". "Chronic health conditions" are also perceived as being driven by "critical change to Earth systems", "natural resource shortages", "pollution", "extreme weather events", "biodiversity loss and ecosystem collapse". A further significant risk associated with the environmental issue is the "economic downturn". This is driven by a number of factors, including "natural resource shortages", "critical changes to Earth systems", "extreme weather events" and "non-weather related natural disasters". (World Economic Forum 2024, 44)

Table no. 2: Ranking by severity of selected global risks, on short and long term, according to *World Economic Forum* survey
Source: (World Economic Forum 2024)

Risks (selection)	Global risks ranked by severity		
	Short term (2 years)		Long term (10 years)
Extreme weather events	2	↗	1
Interstate armed conflict	5	↘	15
Involuntary migration	8	↗	7
Economic downturn	9	↘	28
Pollution	10	—	10
Critical change to Earth systems	11	↗	2
Natural resource shortages	13	↗	4
Biodiversity loss and ecosystem collapse	20	↗	3
Infectious diseases	23	↗	19
Chronic health conditions	27	↗	20
Non-weather related natural disasters	33	—	33
Terrorist attacks	32	↘	34

As in the case of the MSI, "extreme weather events" represent the risk perceived as the most severe by the experts interviewed in the WEF report, and the migration related risk ("mass migration as a result of war or climate change", respectively "involuntary migration"[3]) occupies similar positions in the two rankings (7th in the last edition of MSI, respectively 8th place on short term and 7th place on long term in the WEF). Concurrently, the experts interviewed do not anticipate that the risks of "interstate armed conflict" and "terrorist attacks" will remain elevated in the next decade, a perspective that diverges from that of the surveyed population in the case of the MSI, who perceive these risks as significant (Table no. 1).

The *Special Eurobarometer 538 Climate Change*, conducted in May and June 2023 at the European level, indicates that while the proportion of respondents who view climate change as "the single most serious problem facing the world as a whole"

[3] The link between the two risks can be established on the basis of the WEF definition of involuntary migration, which encompasses factors such as conflict and climate change as potential triggers: "Forced movement or displacement across or within borders. Drivers include, but are not limited to: persistent discrimination and persecution; lack of economic advancement opportunities; human-made disasters; natural disasters and extreme weather events, including the impacts of climate change; and internal or interstate conflict." (World Economic Forum 2024, 97).

has declined from 18% in 2021 to 17% in 2023, it remains a significant concern, following "poverty, hunger and lack of drinking water" (20% in 2023, an increase of three percentage points from 2021) and "armed conflicts" (19% in 2023, an increase of 15 percentage points from 2021, when the war of aggression against Ukraine had not yet commenced) (European Commission 2023, 10). By country, climate change is seen as the world's most important problem in Sweden (41%), Denmark (35%), the Netherlands (35%), Finland (25%), Finland (25%), Ireland (24%), Germany (22%), Malta (22%), Belgium (20%) and Austria (18%). In contrast, only 4% of respondents in Latvia, 6% in Bulgaria, 6% in Romania, 7% in Poland, 8% in Estonia and 8% in Slovakia believe that climate change is the most important problem of the entire world, their attention being directed to the war in the vicinity: 28% of respondents in Latvia, 26% in Bulgaria, 18% in Romania, 37% in Poland, 33% in Estonia, and 22% in Slovakia perceive "armed conflicts" as the single most serious problem facing the world as a whole (European Commission 2023, 12).

Another issue related to climate change, namely the deterioration of nature, is the second most frequently mentioned item only in Hungary (11%) and Slovenia (15%), where the most frequently mentioned problem is "poverty, hunger and lack of drinking water", issues that can also be correlated, under certain conditions, to climate change (Table no. 3).

Table no. 3: Ranking the most frequently mentioned item in EU as "the most serious problem facing the world as a whole", according to *Special Eurobarometer 538. Climate change*

Source: (European Commission 2023)

Problems (selection)	Ranking of the most single serious problem facing the world as a whole		
	March/April 2021		May/June 2023
Poverty, hunger and lack of drinking water	1	—	1
Armed conflicts	8	↗	2
Climate change	2	↘	3
The economic situation	4	—	4
Deterioration of nature	5	—	5
Spread of infectious diseases	3	↘	7
Health problems due to pollution	6	↘	8
International terrorism	9	↘	11

In general, it can be observed that, following the end of the pandemic and the emergence of other potential crises and conflicts (such as war, terrorism and cyber-attacks), the public perception of health risks, including the pandemic coronavirus and future pandemics, has shifted. This is in contrast to the findings of the first edition of the surveys, where these risks were considered to be of greater importance. In contrast, environmental risks and climate change continue to be perceived as of significant importance by the surveyed population, with fluctuations related to geographical location, standard of living and quality of life of the surveyed population, and time frame of the survey.

Brief Conclusion and Suggestions Regarding the Framework for Analysis

The analysis of global risk perception reveals that individuals, regardless of their status or expertise, are aware of the vulnerabilities and challenges associated with climate change. Given the simultaneous occurrence of this phenomenon alongside other events and phenomena with an impact on security, it is imperative to analyse it within the context of the global permacrisis. At the preliminary stage of analysis, the term "permacrisis" must be translated into observable events, thus enabling a situation to be evaluated in terms of indicators pertaining to both objective phenomena (material destruction and human losses caused by climate change, along with economic crisis, migration, refugee flows, internal displacement, etc.) and subjective ones (perceived insecurity, adaptation to the new situation of various social group, including refugees and internally displaced persons, perceived stress, etc.).

A framework for analysis dedicated exclusively to the impact of climate change on the societal dimension of national security must take into account, on the one hand, the correlations with other areas of social life and, on the other hand, the two types of phenomena mentioned above. This is due primarily to the fact that while the analysis of structural data allows for the identification of variables that have been repeatedly associated with losses, risk perception provide insight into intangible aspects that can be exploited in order to add depth to the understanding of vulnerability and risk. While the primary challenge associated with this mixed approach is the potential inconsistency between quantitative and qualitative assessments of vulnerability and risk, it remains a viable methodological option as it provides a comprehensive understanding of the phenomenon, thereby facilitating informed decision-making.

Furthermore, it is crucial to consider the inherent uncertainty associated with the impact of climate change on national security. This applies not only to the societal dimension but to the general analysis as well. Risk, hazards (in terms of frequency and magnitude), exposure, and vulnerability are all characterised by a certain level of uncertainty. A comprehensive approach to the phenomenon could facilitate its

reduction; however, it cannot be eliminated, primarily due to the inherent uncertainty of the future and the complex interdependencies among various domains of social life.

A final point to be made regarding this framework for analysis concerns the question of value at risk. Without the identification of such a value, the analysis is incomplete. The answer to this requirement is dependent on a number of factors, including the specific community or society in question, as well as the historical context. Therefore, it is crucial to consider the role of risk perception in developing future strategies and policies, as it provides a coherent basis for decision-making.

BIBLIOGRAPHY:

Bunde, Tobias, Sophie Eisentraut, Leonard Schütte, and (Eds.). 2024. *Lose-Lose? Munich Security Report 2024.* Munich: Munich Security Conference. Accessed 02 19, 2024. 10.47342/BMQK9457.

Bunde, Tobias, Sophie Eisentraut, Natalie Knapp, Randolf Carr, Julia Hammelehle, Isabell Kump, Luca Miehe, and Amadée Mudie-Mantz. 2022. *Munich Security Report 2022: Turning the Tide – Unlearning Helplessness.* Munich: Munich Security Conference. Accessed 06 15, 2024. doi:https://doi.org/10.47342/QAWU4724.

Cardani, Roberta, Philipp Pfeiffer, Marco Ratto, and Lukas Vogel. 2023. "The COVID-19 recession on both sides of the Atlantic: A model-based comparison." *European Economic Review* 158. Accessed 04 06, 2024. doi:10.1016/j.euroecorev.2023.104556.

Cardona, O.D., M.K. van Aalst, J. Birkmann, M. Fordham, M. McGregor, G. McGregor, R. Perez, R.S. Pulwarty, E.I.F. Schipper, and B.T. Sinh. 2012. "Determinants of risk: exposure and vulnerability." In *A Special Report of Working Groups I and II of the Intergovernmental Panel on Climate Change (IPCC)*, by C.B. Field, V. Barros, T.F. Stocker, D. Qin, D.J. Dokken, K.I. Ebi, M.D. Mastrandrea, et al., 65-108. Cambridge, UK, and New York, NY, USA: Cambridge University Press.

Doise, Willem, and Augusto Palmonari. 1996. "Caracteristici ale reprezentărilor sociale." In *Psihologie socială. Aspecte contemporane*, by Adrian (coord.) Neculau, 23-33. Iași: Polirom.

Duveen, Gerard. 2001. "Introduction: The Power of Ideas." In *Social Representations: Explorations in Social Psychology*, by Serge Moscovici, 1-17. New York: New York Univeristy Press.

European Commission. 2023. "Special Eurobarometer 538. Climate Change." Accessed 06 25, 2024. file:///C:/Users/sarcinschi.alexandra/Downloads/Climate_change_2023_eb538_report_en.pdf

Flynn, Cassie, Silvia Tovar Jardon, Stephen Fisher, Matthew Blayney, Albert Ward, Hunter Smith, Paula Struthoff, and Zoe Fillingham. 2024. *Peoples' Climate Vote*

2024. New York: UNDP. Accessed 06 21, 2024. https://www.undp.org/sites/g/files/zskgke326/files/2024-06/undp-oxford-peoples-climate-vote-2024.pdf

Handmer, John. 2003. "We are all vulnerable." *The Australian Journal of Emergency Management* 18 (3): 55-60.

IPCC. n.d. "Climate change." *IPCC Glossary v 1.5*. Accessed 06 20, 2024. https://apps.ipcc.ch/glossary/

Joffe, Helene. 2003. "Risk: From perception to social representation." Edited by The British Psychological Society. *The British journal of social psychology* 42: 55-73. Accessed 04 12, 2024. doi:10.1348/014466603763276126.

Lo Monaco, Gregory, Anthony Piermatteo, Patrick Rateau, and Jean Louis Tavani. 2017. "Methods for Studying the Structure of Social Representations: A Critical Review and Agenda for Future Research." *Journal for the Theory of Social Behaviour* 47 (3). Accessed 04 16, 2024. doi:http://dx.doi.org/10.1111/jtsb.12124

Machin Suarez, R. 2021. "From Social Perception and Social Representation to Social Imaginary in Social Psychology Theory and Research." In *New Waves in Social Psychology*, by R. Machin Suarez. Palgrave Macmillan. Accessed 04 12, 2024. doi:doi.org/10.1007/978-3-030-87406-3_6

Markova, Ivana. 2004. *Dialogistica și reprezentările sociale.* Iași: Polirom.

Neculau, Adrian. 1996. "Reprezentările sociale - dezvoltări actuale." In *Psihologie socială. Aspecte contemporane*, by Adrian (coord.) Neculau, 34-51. Iași: Polirom.

Prior, Tim, Florian Roth, Linda Maduz, and Flavia Scafetti. 2017. *Mapping Social Vulnerability in Switzerland: A pilot study on flooding in Zurich.* Zurich: Centre for Security Studies. Accessed 04 10, 2024. https://css.ethz.ch/content/specialinterest/gess/cis/center-for-securities-studies/en/publications/risk-and-resilience-reports/details.html?id=/m/a/p/p/mapping_social_vulnerability_in_switzerl

Prunckun, Hank. 2015. *Scientific Methods of Inquiry for Intelligence Analysis.* London: Rowman&Littlefield.

Reisinger, Andy, Mark Howden, and Carolina Vera. 2020. *The Concept of Risk in the IPCC Sixth Assessment Report: A Summary of Cross-Working Group Discussions*. Geneva: IPCC. Accessed 04 12, 2024. https://www.ipcc.ch/site/assets/uploads/2021/01/The-concept-of-risk-in-the-IPCC-Sixth-Assessment-Report.pdf

Seca, Jean-Marie. 2008. *Reprezentările sociale.* Iași: Institutul European.

The Centre for Climate and Security. 2021. *International Military Council on Climate and Security. The World Climate and Security Report 2021*. The Center for Climate and Security. Accessed Octombrie 27, 2021. https://imccs.org/wp-content/uploads/2021/06/World-Climate-and-Security-Report-2021.pdf

The Hague Centre for Strategic Studies. 2012. "D.1.2. A Working Definition of Societal Security." Deliverable submitted in November 2012 (M11) in fulfilment

of the requirements of the FP7 project, ETTIS - European security trends and threats in society. Accessed 04 12, 2023. https://www.researchgate.net/publication/260061753_A_Working_Definition_of_Societal_Security_Final_Deliverable_of_Work_Package_12_Definition_of_Societal_Security_of_European_Security_Trends_and_Threats_In_Society_ETTIS_a_European_Union_Seventh_Framewo.

UN. 1992. "United Nations Framework Convention on Climate Change." Accessed 06 20, 2024. https://unfccc.int/files/essential_background/background_publications_htmlpdf/application/pdf/conveng.pdf

van der Linden, Sander. 2017. "Determinants and Measurement of Climate Change Risk Perception, Worry, and Concern." *Oxford Research Encyclopedia of Climate Change.* Oxford University Press. Accessed 04 16, 2024. doi:https://doi.org/10.1093/acrefore/9780190228620.013.318.

van der Linden, Sander. 2014. "The social-psychological determinants of climate change risk perception: Towards a comprehensive model." *Journal of Environmental Psychology.* Accessed 04 16, 2024. doi:10.1016/j.jenvp.2014.11.012.

van der Linden, Sander. 2015. "The social-psychological determinants of climate change risk perceptions, attitudes, and behaviours: a national study." *Environmental Education Research.* Accessed 04 16, 2024. doi:10.1080/13504622.2015.1108391.

van Diemen, R. 2019. "Annex I: Glossary." In *Climate Change and Land: an IPCC special report on climate change, desertification, land degradation, sustainable land management, food security, and greenhouse gas fluxes in terrestrial ecosystems*, by P.R. Shukla, J. Skea, E. Calvo Buendia, V. Masson-Delmotte, H.-O. Portner, D.C. Roberts, P. Zhai, et al. Accessed 04 12, 2024. https://www.ipcc.ch/report/srccl

van Eck, Christel W., Bob C. Mulder, and Sander van der Linden. 2020. "Climate Change Risk Perception of Audiences in the Climate Change Blogisphere." *Sustainability* 12. Accessed 04 16, 2024. doi:10.3390/su12197990.

Wagner, Wolfgang, Gerard Duveen, Robert Farr, Sandra Jovchelovitch, Fabio Lorenzi-Cioldi, Ivana Markova, and Diana Rose. 1999. "Theory and methods of social representations." *Asian Journal of Social Psychology* (2): 95-125.

World Economic Forum. 2024. *The Global Risks Report 2024. Insight Report.* Geneva: World Economic Forum. Accessed 01 11, 2024. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

DOI: 10.53477/1842-9904-24-7

A THEORETICAL ANALYSIS OF THE ART OF DECEPTION FROM THE 2022 KHARKIV COUNTEROFFENSIVE

George-Ion TOROI, PhD*

The use of deception in military operations has been a key tactic throughout history, and the 2022 Kharkiv counteroffensive provides a fascinating case study in the art of deception in warfare. This essay delivers an in-depth analysis of the various deceptive tactics employed during the counteroffensive, including concealment of troop maneuvers, misinformation campaigns, and feint attacks. By examining these tactics in detail, the study aims to shed light on the effectiveness of deception in current military operations and to draw lessons for future operations planning. The approach of the case study presented facilitated a comprehensive understanding of how deception was used in the 2022 Kharkiv counteroffensive, while also facilitating the identification and confirmation of key enduring principles, types, and methods of deception employed by the military forces involved. The essay also sets the stage for discussing the particularities of military deception from a theoretical point of view and how it was employed in the operation, but also its impact on the outcome of the Kharkiv campaign.

Keywords*: deception; surprise; counteroffensive; perception; operational advantage.*

Introduction

Deception, particularly in the realm of information operations, is a multifaceted phenomenon that involves the intentional creation of misperceptions to achieve specific goals. The art of deception has been a crucial element in military strategy throughout history, allowing commanders to deceive their enemies and gain the upper

**** Lieutenant-Colonel George-Ion TOROI, PhD, is a Senior Instructor within the Command and Staff Faculty, "Carol I" National Defence University, Bucharest, Romania. E-mail: george_toroi@yahoo.com***

hand. However, considering the technological evolution of the intelligence collection sensors nowadays, there are voices that question the effectiveness deception tactics. Regardless of becoming more challenging and complex, The Russian-Ukrainian conflict has demonstrated in numerous instances that this is not the case (Russian War Against Ukraine. Lessons Learned Curriculum Guide 2023, 27). Deception has been a longstanding tactic used by both sides throughout the entire conflict so far.

The human mind is the target of deception and regardless of technology it remains susceptible to deception (Michael Bennett 2007, 12). Deception operates on the fundamental principle that humans can be influenced by false information or manipulated through psychological tactics exploiting their vulnerabilities and cognitive biases.

The 2022 Kharkiv counteroffensive was a significant military operation focused on regaining some of the Russian occupied territories in the Kharkiv region, inflicting heavy casualties on the enemy and boosting the Ukrainian morale. The operation involved a complex array of tactics and strategies, some considering it a German blitzkrieg reminiscent (Shandra 2022). The operation was also characterized by a high level of deception, which played a vital role in shaping the outcome of the military campaign. The remarkable success of the Ukrainian operation emphasizes the fact that "deception must be an integral part of all operations" (Planning and Execution Handbook 2018, 6-2). By analyzing the tactics and techniques used during this counteroffensive, we can gain valuable insights into the effectiveness of deception in warfare.

After the failed Russian invasion at the beginning of the conflict, the fighting along the front has largely degenerated into a grinding war of attrition. However, on September 6th, 2022, Ukrainian forces launched a bold counteroffensive in the vicinity of Kharkiv that swiftly turned into an astounding triumph. In only six days, Ukrainian forces recaptured an area of about 6,000 square kilometers and advanced up to 70 kilometers into Russian-held territory, posing a threat of encirclement, driving Russian forces from the area, and seizing a sizable quantity of Russian military munitions and equipment (Ryan 2022). Balakliya, Izium, or Kupiansk, among others have all been recaptured as a consequence of this counteroffensive. However, this could not have been possible without the coordinated efforts of Ukrainian military leaders and the effective use of deception tactics to surprise the Russian forces and gain a strategic advantage.

The 2022 Kharkiv counteroffensive serves as a prime example of deception operation; therefore, we consider it is crucial to delve into the various strategies and tactics employed in support of its objectives to understand the art of deception in contemporary warfare. To this end, the paper analyzes the theory of deception and its application in the context of the counteroffensive. The article serves as an entry point for outlining the perpetual nature of deception and its impact on military

operations. It also highlights the necessity of understanding deception in modern warfare considering its importance and relevance regardless of the modern transparent battlefield. Moreover, it offers a theoretical analysis that examines various tactics and techniques employed, shedding light on the intricacies of deception in warfare.

Problem statement and aim of the study

Regardless of its strategic importance, the 2022 Kharkiv Counteroffensive remains an understudied subject. Many of the available sources primarily focus on the military aspects of the operation, leaving the art of deception largely unexplored. For this reason, the lack of comprehensive analysis on the tactics and psychological aspects of deception used during the counteroffensive represents a significant gap in current military studies. Consequently, it is imperative to conduct a thorough examination of the deceptive strategies employed to gain a deeper understanding of the complexities involved. As such, the aim of this paper was to address this gap by providing a theoretical analysis of the art of deception from the 2022 Kharkiv Counteroffensive.

Methodology

To fulfil this aim, we have conducted a qualitative analysis to better understand the intricacies of deception used in the Kharkiv Counteroffensive, the findings of this analysis having the potential to provide valuable insights into the strategic use of deception in current military operations. In accordance with this approach, we have used an inductive reasoning in order to generate valid and reliable conclusions based on the data collected (Lisa M. Given, 2008, p. 429). It is recon that most of the qualitative studies make use of an inductive reasoning process (John W. Creswell, 2023, p. 276). As a consequence, it was not a hypothesis testing study, but rather a research question driven. Consequently, the main research question that guided the study was: *How did the 2022 Kharkiv counteroffensive use the theory of deception to achieve its objectives?*

In line with the methodological options previously presented, we have employed a case study strategy to investigate the art of deception employed during the 2022 Kharkiv Counteroffensive. Due to the limitations of an ongoing conflict, we have only employed secondary data from various sources that monitors the evolution of the conflict. However, their importance in research is well acknowledged in the academic community (Walliman, 2022, p. 102). We have adopted a historical approach analyzing the chronological events that led to the surprising Ukrainian counter offensive on September 6th, 2022. Further-on, we have interpreted all these from a deception theory perspective, identifying key deception indicators and events, but also specific tactics and procedures the Ukrainians employed.

The potential value of the study and its target

The results of the study can have multiple benefits: enhancing military knowledge on a subject critical to the operational success in today's confrontations, ensuring a deeper historical documentation, but also providing an educational tool that could be used in training and educational programs, to mention just a few of the potential impacts of this analysis that highlights its value. As such, the target audience of the article can be military commanders and planners, but also academic institutions and researchers interested in the art of deception and its impact on military strategies.

Paper structure

To address the main research question and fulfil the aim of the study we have structured this paper in three main parts. The first part provides a theoretical analysis of deception operations, the second part examines the historical context of the 2022 Kharkiv Counteroffensive and the third part offers an analysis of this operation from a theoretical deception perspective.

1. A Short Theory of Deception

"No major operations should be undertaken without planning and executing appropriate deceptive measures" (AFM 2018, 3A-1). Thus, understanding the intricacies of the art of deception in warfare is crucial for maximizing the success of military operations. As such, the aim of this section is to provide a brief overview of the key concepts and principles of deception in warfare.

As previously mentioned, deception has been a part of military strategy for centuries and a key component in achieving victory on the battlefield (Friedman 2017, 73). The numerous advantages it can provide for military commanders make it an indispensable tool for achieving victory on the battlefield. Reducing casualties, providing freedom of movement, and enabling surprise attacks are just a few of the benefits deception offers that may increase operational success during military endeavors (Robert M. Clark 2019, 36) (Lyndon Benke 2021, 76).

Deception implies the deliberate act of misleading or tricking targeted enemy decision-makers into believing something that is not true and behave in a way that is contrary to their best interests, in support of the deceiver objectives. The purpose of deception is to mislead the adversary and cause them to misinterpret the operational situation by creating confusion and uncertainty. Moreover, deception operations should have a clearly defined target, which is the adversary's decision-making body that has the appropriate power to generate intended enemy behavioral change. The outcome of this change should facilitate a favorable position for the deceiver, by portraying operational advantages on the battlefield in their favour.

The success of deception hinges on the ability to manipulate information and perceptions to induce a desired response from the target audience. Deception

operations should also be planned and executed in a way that exploits the adversary's cognitive biases and decision-making processes. When properly employed, deception can be a powerful tool in military strategy. It may be used to influence the enemy OODA loop (Observation, Orientation, Decision, Action) in order to slow down the enemy and disrupt their decision-making process, ultimately creating opportunities for exploitation. Figure no. 1 illustrates key common themes within the deception literature with respect to its definition.

The first step in incorporating deception in the overall concept of operations is to define its potential goals and objectives. The goals are those intended operational effects that deception can achieve in support of the military operation, and may include diverting enemy attention, concealing true intentions, achieving surprise, ensuring freedom of action or inducing the enemy to make incorrect assumptions about friendly forces by creating confusion among its forces. It is also important to note that the goals of deception can vary depending on the specific operational circumstances, but they are always designed to support the friendly operation in some way.

Deception objectives, on the other hand, focus on the external conditions. They reflect the enemy intended reaction to the false indicators portrayed by the deceiver. In other words, the objectives reflect what the enemy needs to do in order for the deception goals to be fulfilled. For example, if the enemy needs to redirect their forces to a specific location, the deception goals would be to make them believe that the main attack is coming from that direction.

Moreover, one should carefully consider the employment of deception. It is essential to understand the potential impact on both the enemy's and our own operation. A risk analysis process should also be conducted to identify potential vulnerabilities and mitigate them before they can be exploited by the enemy. If deception is not suitable in the respective operational circumstances, or is too risky and the benefits are few, it may be more advantageous to disregard its employment. In such cases, alternative strategies should be considered to achieve the desired operational outcomes. However, if it is assessed that deception is suitable, then a detailed plan for implementing it must be developed. This should start with designing achievable goals and objectives for the deceptive operation, which represent the bedrock for any deception plan, ensuring that they align with the overall strategy and are realistic given the resources available.

After this step is paramount that a desired enemy perception is set. This concept plays a crucial role in the art of deception as it represents a fundamental aspect of manipulating the target audience's beliefs and actions, thus allowing the objectives to be achieved. This enemy false representation of reality is what shapes their choices and actions. One can notice the crucial role that the enemy's desired perception plays in achieving the deception objective.

This concept is closely related to the target of deception. It aims to create a desired perception in the target's mind. The art of deception is used to manipulate the target's understanding of the situation. It can shape the desired perception and lead to certain actions or inactions. This perception can be influenced by various factors such as the information presented, the communicator's (channel) credibility, or the emotional appeal of the message. Personal experiences and biases, but also societal and cultural norms can also play a significant role in shaping the desired perception. All these factors can greatly influence the way individuals perceive and interpret information; thus, a proper analysis of the target is very important in the deception process.

Once the goals, objectives and desired perception of the enemy have been established the next step is to devise a strategy to shape the narrative. It is the time to properly select the most effective techniques, methods, types, tactics and means of conveying the desired message in order to mislead or confuse the enemy.

According to the literature, the two types of deception are: A-type and M-type, both make use of one of the key enduring features of the nature of warfare, uncertainty. A-type, or ambiguity producing deception focuses on creating confusion by increasing uncertainty and doubt in the enemy's mind by overloading the enemy intelligence process with information or by employing conflicting information to make it difficult for them to make accurate decisions. Creating multiple plausible scenarios for the enemy to consider and react to, A-type deception is used to sow seeds of doubt and hesitation. On the other hand, M-type deception, also known as misdirection deception, aims to lead the enemy into believing a certain reality that is actually false. It involves planting false information or using dummy equipment, but also creating diversions to distract the enemy attention, determining them to act in a way that benefits the deceiving party. These diversions can take many forms, such as feigning an attack or spreading disinformation through various channels, as we shall see, happened in the 2022 Kharkiv counteroffensive (Bouwmeester 2021, 425-426).

Furthermore, there are two main methods of deception: simulation and dissimulation. Simulation involves creating a false appearance, while dissimulation involves concealing the truth. Both methods are used in military tactics to mislead and confuse the enemy. The goal of simulation is to create a false impression of the size, strength, position of forces, or timings of friendly actions, that the enemy will act upon, leading to operational advantages for the deceiving force. Similarly, dissimulation involves actively concealing the true nature of one's actions or intentions, leading the enemy to make incorrect assumptions. Each of the two, according to some specialists, have three sub-methods. As such, simulation can be achieved through masking (concealing the true nature of an object), repackaging (altering the appearance of an object), and dazzling (obscuring the true nature of an

object), while dissimulation can be accomplished by mimicking (imitating another object), inventing (creating a false appearance) and decoying (creating a false target). All of these methods of deception are crucial in military strategy and have been used throughout history to mislead and confuse enemies.

In addition to these methods, there are several specific tactics appropriate to each of the two big methods that can be employed for deception in warfare (George-Ion TOROI 2023, 27). As simulation involves creating fake or false information to mislead the enemy, display, feint, demonstration or disinformation are commonly used tactics. On the other hand, dissimulation involves hiding true intentions or capabilities through camouflage and concealment, but also denial. All these tactics are critical to the success of military operations and can be seen throughout history in various battles and campaigns. It is worth noticing that using it in combination can increase the effectiveness of the deception tactics employed. The use of simulation and dissimulation together can enhance the effectiveness of the deception tactics employed.

Moreover, several recognized techniques present how deception can be utilized to manipulate the adversary's perception of reality and create the desired operational advantage on the battlefield. Some examples include presenting to the enemy an obvious solution that they believe to be true and reinforcing their false perception, conditioning them to expect a certain response by repeatedly demonstrating a pattern of behavior that lulls the enemy into a false sense of security, suppressing the force signature in order to confuse the enemy regarding the size, location and future actions of friendly forces, or to lure the enemy in what they believe to be the proper reaction.

The means of deception represent specific resources used to execute the deceptive actions that convey the message to the enemy. These are either physical, technical or administrative. Physical means include tangible resources such as camouflage or dummy equipment. Technical means involve the use of technology for communication, interception and creating false electronic signals. These can include cyber-attacks, electronic warfare, and signal jamming. Administrative means imply spreading false information or using forged documents to mislead the enemy.

Once the proper type, methods, tactics, technics and means have been carefully selected, the art of deception can be effectively employed to achieve the desired outcome. To this end, a specific deception story that incorporates multiple events to convey the deceptive message to the enemy collection assets must be constructed with precision and executed with utmost care and attention to details. Creating a convincing narrative and controlling the flow of information is essential for successful deception operations. This requires a deep understanding of the enemy's cognitive biases and current situational awareness, but also a thorough analysis of

its intelligence capabilities and the likely responses to minimize any risk. When developing the entire scenario, it is recommended to consider the principles of deception. These will help structure deception story to maximize effectiveness and minimize the risk of detection. Understanding the principles of deception is essential in effectively implementing strategic tactics and achieving success in military operations.

An important concept in this respect is selecting the proper deception channels. These represent the specific pathways through which the enemy receives the false information. Considering the features of the current information environment, social-media has become a significant channel of deception, allowing for the spread of misinformation and propaganda at an unprecedented rate. This has led to a blurring line between truth and fiction, making it difficult for the public to discern what is real and what is not. Moreover, this channel can have far-reaching consequences, shaping public opinion and influencing political decisions.

History has demonstrated that deceptive tactics can be employed through various channels of communication such as double agents or diplomatic assets, but the most important one is the enemy intelligence collection sensors. NATO recognizes six intelligence disciplines (AJP-2 Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security 2020, 3-1 - 3-2) all of which playing a crucial role in delivering the intended message. These include ACINT (Acoustic intelligence), HUMINT (Human intelligence), IMINT (Imagery intelligence), MASINT (Measurement and signature intelligence), OSINT (Open-source intelligence) and SIGINT (Signals intelligence). Each discipline provides unique opportunities for deception and can be employed in different ways to mislead the enemy.

When selecting the channels of deception, it is crucial to understand that time is an important factor. It is of utmost importance to deliver a message in a form that the enemy can decipher, but also at a moment when its collection asset is likely to detect it. Moreover, in order to increase the chances of the deception success, the deceiver must carefully exploit any potential weaknesses in the enemy's intelligence network. It is also advisable to synchronize the deceptive message across multiple channels of communication.

To sum up, the entire theoretical model presented in this section provides a sound framework for analyzing and understanding the art of deception in the context of the 2022 Kharkiv counteroffensive. However, in order to fully comprehend the intricacies of deception employed during the operation, one should first consider the operational context up to and during the counteroffensive, which we will present in the next section. This will provide a comprehensive understanding of the strategic and tactical elements at play.

2. The 2022 Kharkiv Counteroffensive: Overview

The Russian invasion of Ukraine started on February 24th, 2022, has transformed into a full-scale military conflict which has been going on for several years now. What should have been a three-day engagement (N. R. Jack Watling 2022, 1) has turned into a prolonged and devastating war of attrition, resulting in significant loss of lives and widespread destruction, without a foreseeable end. "It is the largest conventional armed conflict in Europe since World War II" (Koffman 2024, 99).

Multiple inaccurate planning assumptions, bad tactical coordination and logistic support, but also undermining the Ukrainian response led to significant setbacks for the Russian forces during the initial phase of the conflict. As a result, the Russian forces faced unexpected resistance and suffered heavy casualties. It is acknowledged that "soldiers defending their own homes and families are far more motivated than invaders" (David Petraeus 2023, 334). Counting on the support of international allies, the Ukrainian military successfully repelled the Russian advance from seizing the two big cities in the country, Kiev and Kharkiv, and ruined Russian plans to quickly overthrow the Ukrainian government. The successful defence was a turning point in the conflict, demonstrating the resilience and determination of the Ukrainian forces. Russians were forced to retreat by the end of March from Kyiv, Sumy and Chernihiv regions (Nathan Hodge 2022), and by May they were pushed back to the border, in Kharkiv (Ukrainian forces in Kharkiv reach Russian border 2022) (Ryan 2022).

After these setbacks, Russia shifted its focus towards Donbas (Mykhaylo Zabrodskyi 2022, 34-43) (Koffman 2024, 111), making up for a manpower shortfall with a 12:1 superiority in artillery fire. During this time, they shot almost 20,000 rounds on average every day (Franz-Stefan Gady 2024). A grinding war of attrition and massive artillery duels characterized this period of the conflict (Koffman 2024, 99). The constant bombardment took a toll on both the soldiers and the civilian population.

As Ukrainian forces were outgunned and out of ammunition, the number of casualties increased. Western support became essential at this point. The Ukrainian forces were in desperate need of assistance. And starting with April 2022 it came, especially in the form of precision-guided missiles and long-range artillery. This allowed the Ukrainian forces to disrupt Russian supply lines and communications, weakening the enemy's ability to coordinate and sustain their operations, and ultimately helping to stabilize the front lines.

Regardless of some advancements in the East Front, Russian forces continued to face heavy resistance from Ukrainian defenders and were halted in their attempts to make significant progress in the Donbas region (O. V. Jack Watling 2024, 7), being forced to resort increasingly to defensive actions (Dmytro Kruhliak 2023). The Ukrainian defenders, despite being outnumbered and outgunned, displayed remarkable resilience and determination.

A critical detail in the development of the conflict was the arrival of the rocket artillery system (HIMARS) (Porter 2022) in late June 2022, which provided the Ukrainian forces with increased firepower and strategic advantage. This allowed for an extension of the operations in the south, in Kherson, adding pressure on the Russian forces, which was an essential element in support of constructing later-on the deception story for the Kharkiv counteroffensive.

However, both Kharkiv and Kherson were of critical importance to Ukraine. It was never a question of choosing between them, but rather how to exploit Russian vulnerabilities into regaining them both. Kherson was never of secondary importance to Kharkiv for the Ukrainians (Freedman 2022). The city's strategic location and importance in the region made it a key target for both sides. For the Ukrainians, getting it back was crucial in order to regain control of the region and stop Russians' advancement towards Odessa. Moreover, the region could become a strategic foothold from which to launch further offensives against the Russian forces in order to recapture Crimea, which was annexed by Russia in 2014 (Ryan 2022). Moreover, the region's economic importance and geographic position cannot be overstated. The Russian perception on the location of the next Ukrainian main effort was greatly influenced by these factors.

The plan for the counteroffensive was quite simple. Make the enemy believe that Kherson will be the location for the attack, thus determining them to reinforce this defensive position, while leaving Karkiv less defendable, where the actual offensive will take place. This strategic deception was a key element in the success of the Kharkiv counteroffensive, as it allowed for the element of surprise and caught the Russians off guard.

After many prior events to make the Russian believe Kherson will be the counteroffensive location, on August 29th, President Zelenski actually announced this southern operation, contributing to the reinforcement of the Russian perception. The Ukrainian forces used various tactics and strategies to achieve this, all of which will be analyzed in the next section of the paper.

As a consequence of this shaping operations the Russian forces moved many of their experienced units to deal with the threat posed by the Ukrainian forces in Kherson, leaving the defence of the north-eastern areas weakened (Freedman 2022) (Russia's War in Ukraine: Military and Intelligence Aspects 2022, 22). This led to a significant shift in the balance of power in the Kharkiv region and set the stage for the subsequent events of the counteroffensive, which started on September 6th (Ukraine's southern offensive 'was designed to trick Russia' 2022). The Ukrainian forces launched a coordinated attack against the Russian invaders, resulting in a rapid advancement of the Ukrainian forces, being able to recapture Balaklia, Kupyansk and Izium in just a couple of days. The success of the counteroffensive was largely attributed to the strategic deception employed by the Ukrainian military. The surprise

attacks caught Russian forces off guard and inflicted significant casualties, allowing the Ukrainian troops to gain significant ground as it can be seen in the Figure no 1.

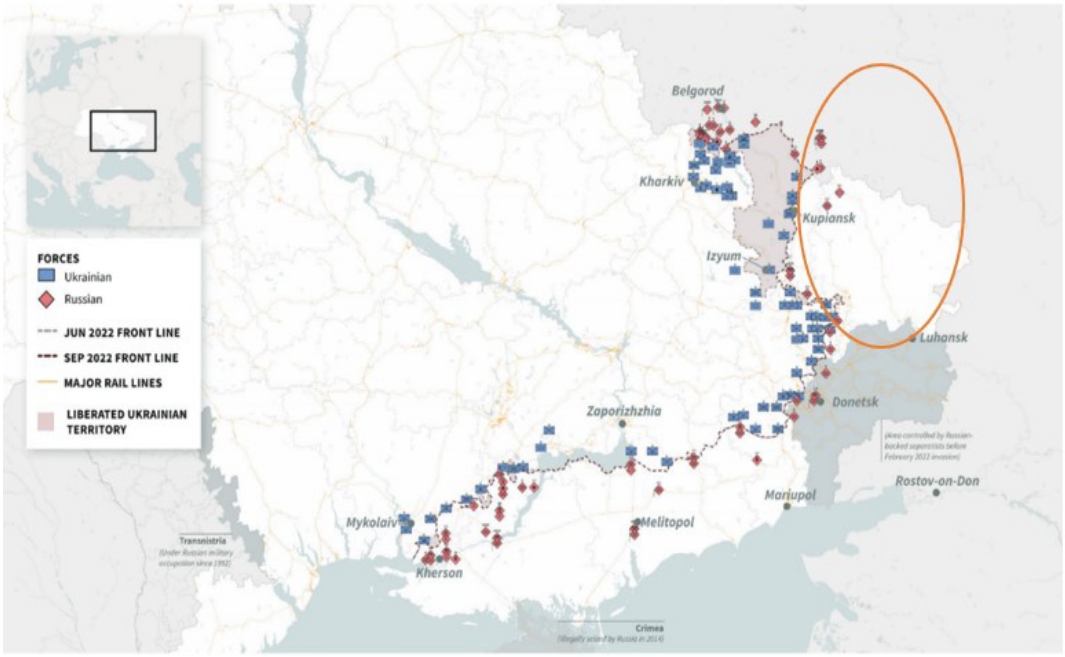


Figure no 1: Operational situation after the Kharkiv counteroffensive (Seth G. Jones 2023, 19)

The counteroffensive has proven to be a turning point in the conflict, with significant implications for its future, some calling it the masterpiece of Ukrainian military actions (Ioniță 2023, 43). Deception has been an essential element in recapturing Kharkiv and subsequently Kherson (Nagl 2024, 51), the surprise being one of the main factors of success (Dmytro Kruhliak 2023). Moreover, it is said that the surprise attack was planned in the same simulation center as the 2003 invasion of Iraq, in Germany (David Petraeus 2023, 368).

The main consequences of this magnificent operation demonstrate the high level of success of the Ukrainian 2022 Kharkiv counteroffensive. Regaining some lost territory, bolstering the Ukrainian morale (Freedman 2022), consolidating international support (Isabelle Khurshudyan 2022) are only a few of them. As for the Russians, beside losing the momentum on the battlefield for the rest of the year, after this embarrassing retreat, Putin declared partial mobilization acknowledging the personnel shortcomings and seeking ways to regain the initiative on the battlefield (Ryan 2022). Also, on October 8th, Putin designated general Sergei Surovikin the first sole commander to lead Russia's war across the entire theater.

To sum up, it is evident that the use of deception played a crucial role in the success of the 2022 Kharkiv counteroffensive. In the next section, we will do a theoretical analysis of the events that shaped the success of the counteroffensive.

3. Main Results of the Theoretical Analysis of Deception in Support of the 2022 Kharkiv Counteroffensive

The art of deception has been a significant strategy in warfare throughout history, and the 2022 Kharkiv counteroffensive provides a compelling case study for understanding its theoretical underpinnings. The Ukrainian operation has demonstrated that "the more successful the deception in support of a plan, the greater the chance the plan will be successful" (Robert M. Clark 2019, 35). This was a strategic deception planned and coordinated at the highest levels of military command and approved by the president himself, according to a report written after interviewing most of the military commanders involved, including the mastermind of the operation, Colonel General Oleksandr Syrskyi (Isabelle Khurshudyan 2022).

In this section, we will analyze the theoretical concepts presented in the first section of this article in the context of the deception operation in support of the Kharkiv counteroffensive. First of all, it is important to understand whether this was indeed a deception. In this respect, after analyzing the theoretical definition and comparing it to the events of the 2022 Kharkiv counteroffensive, we have come up with the following results:

− the events prior to the Kharkiv counteroffensive had the purpose to mislead the Russians making them misinterpret the situation. Moving many of their assets in the southern front to respond to the fictious threat created by the Ukrainians there, thus weakening their positions in the north-east is a clear indicator of the effectiveness of the Ukrainian strategic deception;

− the primary target of the operation was the Russian military-political leadership (Kharuk 2023);

− believing the threat in the south and acting upon it means that the events prior to the counteroffensive have created a behavioral change for the Russians;

− the outcomes of this events have created operational advantages for the initiator which resulted in significant territorial gains.

After this analysis, we can definitely conclude that the events prior to the 2022 Kharkiv counteroffensive were part of an elaborate and sophisticated plan to deceive and mislead the opposing forces, thus ensuring a strategic advantage for the Ukrainians.

Further-on, we will do an analysis of the deception story that had unfolded before the 2022 Kharkiv counteroffensive. As previously mentioned, the story was quite simple. Make the Russians believe that the Ukrainian counteroffensive will

come from the south, in the Kherson region, act upon it, and then launch the actual offensive from the north-east, in Kharkiv region, catching them off guard (Freedman 2022). As such, the most likely goal of deception was to regain the initiative and surprise the Russian forces in the north-east front, thus ensuring freedom of action for the Ukrainian forces in their offensive operation to regain control over the territory in this area, lost during the initial stages of the conflict. Subsequent deception objectives in achieving this goal included:

− Russian forces will redeploy forces and equipment to reinforce their positions along the southern front;

−Russian forces will redeploy their forces and equipment from the north-east or nearby locations that could have affected the Ukrainian counteroffensive in Kharkiv, leaving the area vulnerable to attacks;

− Russian forces will ignore Ukrainian offensive preparation in the Kharkiv region.

In order to accomplish these objectives, the Ukrainians had to create the following desired enemy perception: there will be one single Ukrainian counteroffensive in the near future, in Kherson area, while, at the same time, there is no imminent threat in the Kharkiv region.

In table no. 1 we have summarized the key deceptive events that led to the success of the 2022 Kharkiv counteroffensive. In the same table, where needed, we have also offered interpretations in accordance with the theory of deception.

As part of the deception story, in order to make the enemy believe that there was no real threat coming on the Kharkiev front, the Ukrainians took some effective measures to conceal their true intentions and hide their actual preparations for the counteroffensive. According to a military source with knowledge of the operation, an essential part of it comprised locating informants in Kharkiv areas under Ukrainian control to prevent them from providing the Russians with information on Ukraine's preparations (Ukraine's southern offensive 'was designed to trick Russia' 2022). Furthermore, The Ukrainian reconnaissance started to collect information in the area that helped them better prepare the attack, whilst, at the same time, did some counter-reconnaissance missions to deny the Russian access to real information that would have compromised the counteroffensive preparation (Ryan 2022) (Strachan 2022). This was a success as "the local Russian command failed to pick up any signs of the impending assault" (Freedman 2022). Figure no. 2 highlights how successful the Ukrainians were in hiding their troops. It is a representation of the forces display in the Kharkiv region before and right after the counteroffensive started. One can easily notice that there were no indicators of an imminent attack in the region, Ukrainian forces being perfectly concealed.

Table no 1 Key deceptive events that led to the success of the 2022 Kharkiv counteroffensive

Date	Event	Interpretation
July 09, 2022	Statement made by Iryna Vereshchuk, Ukraine's Deputy Prime Minister in charge of temporarily seized territories, urging the residents to leave Kherson and Zaporizhia provinces. This communication raised concerns about an imminent military operation in the region. (Plokhy 2023, 211)	- using the media and diplomatic channel of communication.
July 10, 2022	Oleksii Reznikov, the Ukrainian Defense Minister announced in media the coming counteroffensive: "The president has given the order to the supreme military chief to draw up plans (Zelensky ordered to reconquer the south of Ukraine - Reznikov 2022)	- using the media and diplomatic channel of communication.
July 12, 2022	In Melitopol, a major transportation hub on the left bank of the Dnieper, witnesses saw columns of Russian vehicles moving towards Kherson. (Russian Offensive Campaign Assessment, July 12 2022)	- positive feedback on creating the desired perception for the Russians.
July 13, 2022	The Russian military started fortifying the routes leading up to the Antonivka highway bridge, east of Kherson city. Additionally, they increased the quantity of patrols in Kherson area. (Russian Offensive Campaign Assessment, July 13 2022)	- positive feedback on creating the desired perception for the Russians.
July 19, 2022	Ukrainian attacks on the three bridges over Dnieper in Kherson area started (the railway and highway bridges at Antonivka, located north of Kherson, and the bridge that links Nova Kakhovka with the Beryslav region near the Kakhovka Dam). Using HIMARS the Ukrainian delivered the first significant attack on the Antonivka highway bridge, devastating both the structure and the nearby fortifications. (Russian Offensive Campaign Assessment, July 19 2022) A lengthy essay in the English-language Kyiv Independent suggested that the two Antonivka bridges – the highway and railway bridges, as well as the Kakhovka Dam Bridge had to be destroyed in order for a counteroffensive to be successful. (Ponomarenko 2022)	- creating the false threat.
July 20, 2022	Sergei Lavrov, Russian Foreign Minister, issued a statement declaring that his country's ambition is no longer limited to Lugansk and Donets, but extends to Kherson and Zaporizhia as well. (Trevelyan 2022)	- positive feedback on creating the desired perception for the Russians.
July 26, 2022	New HIMARS attacks on the bridge, rendering heavy machinery unsuitable to cross it. (Video from Antonivka Road Bridge in Kherson shows extensive damage 2022). The Russians tried initially to repair it but, after another hit in August, decided to install a pontoon bridge, which was also targeted by the Ukrainians. (Axe, The Bridge Battle In Southern Ukraine Is Escalating 2022)	- conditioning enemy perception towards the false location of the attack; - the installation of the pontoon bridge was a feedback indicator of the successful deception story so far.
July 27, 2022	Oleksii Danilov, the secretary of the Ukrainian Defence Council, revealed that the Russian troops had significantly repositioned to the south, specifically towards Kherson, and he speculated that this may be to halt the Ukrainian counteroffensive. (In the Kherson direction began "very powerful" movement of Russian troops - Danilov 2022)	- reinforce the enemy perception that its response is good; - using the media and diplomatic channel of communication.

July 30, 2022	Ukranians hit the Antonivka railway bridge over the Dnipro at Kherson, making Russian forces unable to resupply, by rail, their positions on the west bank of the river. (Russian Offensive Campaign Assessment, July 30 2022)	- reinforcing the false threat.
August 01, 2022	Russia is transferring forces from the east (Slovyansk) to reinforce the southern effort and prepare the defence for the Ukrainian announced counteroffensive. (Russian Offensive Campaign Assessment, August 1 2022)	- positive feedback on creating the desired perception for the Russians.
August 02, 2022	Russia continues to redeploy forces to Kherson (airborne troops from Donetsk). (Russian Offensive Campaign Assessment, August 2 2022) Russian forces continued, throughout August, to transfer forces and equipment to counteract the Ukrainian announced counteroffensive in Kherson.	- positive feedback on creating the desired perception for the Russians.
August 09, 2022	Russian airbase close to Saki, in Crimea, was struck by Ukrainian missiles. Ten Russian planes, the backbone of the air force of the Russian Black Sea Fleet, were destroyed as a result of the strike, which also blew a weapons storage on the airport. (Ukraine claims responsibility for Crimea attacks 2002) (Plokhy 2023, 216) Despite assertions by Western sources of a planned Ukrainian counteroffensive in Kharkiv area, the Ukrainian General Staff did not mention anything of the subject in its evening report. (Russian Offensive Campaign Assessment, August 9 2022)	- reinforcing the false threat. - dissimulation effort on the Ukrainian side.
August 11, 2022	Ukrainian strikes Russian command posts and also ammunition depots in the Southern area. (Russian Offensive Campaign Assessment, August 11 2022)	- reinforcing the false threat.
August 17, 2022	Western sources record that Russian mass redeployment of troops and equipment from Donbas and Crimea to Kherson in preparation for the Ukrainian counteroffensive. It is assessed that Russia has 30 BTG on the river's right bank. (Ukraine Strategy Targets Russian Army's Lifelines in Kherson 2022) Consequently, concerns were raised by Ukrainian officials regarding the decision to announce the counteroffensive.	- positive feedback on creating the desired perception for the Russians. - reinforcing enemy false perception.
August 20, 2022	Ukrainians continue to strike enemy positions and ammunition depots in Kherson. (Russian Offensive Campaign Assessment, August 20 2022)	- reinforcing the false threat.
August 23 - 26, 2022	Ukrainians continue to disrupt enemy activities in Kherson region by targeting GLOCs (ground lines of communication). (Russian Offensive Campaign Assessment, August 24 2022)	- reinforcing the false threat.
August 29, 2022	President Zelenski announced the beginning of the counteroffensive in Kherson. (President of Ukraine 2022) Other officials reinforce the location for the counterattack, but also the full commitment of the Ukrainian people. (Ukrainian adviser warns progress will be slow as southern counterattack begins 2022) The media around the world reiterated the beginning of the counteroffensive in Kherson contributing to the enhancement of the disinformation campaign. (Ukraine's southern offensive 'was designed to trick Russia' 2022)	- reinforcing the false threat. - using the media and diplomatic channel of communication.

September 02, 2022	Sergei Shoigu, Russian Defence Minister, stated that "this action was planned by Zelensky's office with one single goal—to give their Western sponsors the illusion of the Ukrainian Armed Forces' capacity to manage an assault." (Shoigu announced the attempts of the APU to the Nikolaev-Kryvorozhsky and other directions 2022)	- positive feedback on creating the desired perception for the Russians.
September 03, 2022	The Kakhovka dam bridge was severely damaged by the Ukrainians, a great part of it collapsing into water.	- reinforcing the false threat.
September 04, 2022	Ukrainians made some local gains from the start of the counteroffensive, targeting Russian command posts, GLOCs or logistic depots. (Russian Offensive Campaign Assessment, September 4 2022)	
September 06, 2022	Russians redeployed forces from north-east to reinforce the defensive line in Kherson, formations from one of its best army's unit, the 1st Guards Tank Army (GTA), being spotted in the area. (Axe, Russian Troops are Dashing around Ukraine Trying to Block Ukrainian Counterattacks. 2022) Only Russian volunteer forces and activated reservists from the "people's republics" of Luhansk and Donetsk manned the Russian positions in Kharkiv region. (Trofimov 2024, 268). Based on American intelligence, the Ukrainian found out that only half of the Russian units were still stationed in that area as opposed to a month before. (Isabelle Khurshudyan 2022) At the same time, Ukrainians launched the real counteroffensive in Kharkiv region. The five brigades conducting the attack were reinforced with some of the best Western weapons' systems. This was a concealed operation that had happened across the previous weeks. (Ukraine's southern offensive 'was designed to trick Russia' 2022) (Isabelle Khurshudyan 2022) Ukrainian forces advanced very easily because of the effects of surprise on the Russians and the lack of a coordinated response on their side.	- positive feedback on creating the desired perception for the Russians. - positive feedback on the success of the deception story.

From the course of the events presented, it is obvious that the Ukrainians pulled an M-type deception, in order to mislead the Russians into believing that the counteroffensive will take place in the Kherson area. This strategic move allowed the Ukrainian forces to successfully execute their planned counteroffensive.

As for the deception methods, one can notice that the Ukrainians employed both simulation and dissimulation in order to mislead the enemy forces. It is a fact proven by history that the use of simulation and dissimulation combined can be extremely effective in military operations. Simulation involves creating a false appearance, which the Ukrainians did with the false counteroffensive in Kherson, while dissimulation involves concealing true intentions or capabilities as they did in Kharkiv region prior to the real attack. This employment of both these methods was highly effective allowing the Ukrainian forces to gain a strategic advantage over the Russian forces.

In accordance with these methods, several tactics were employed:

Display. Portraying more troops in the Kherson area to distract Ukrainian forces and draw attention away from the real target in Kharkiv.

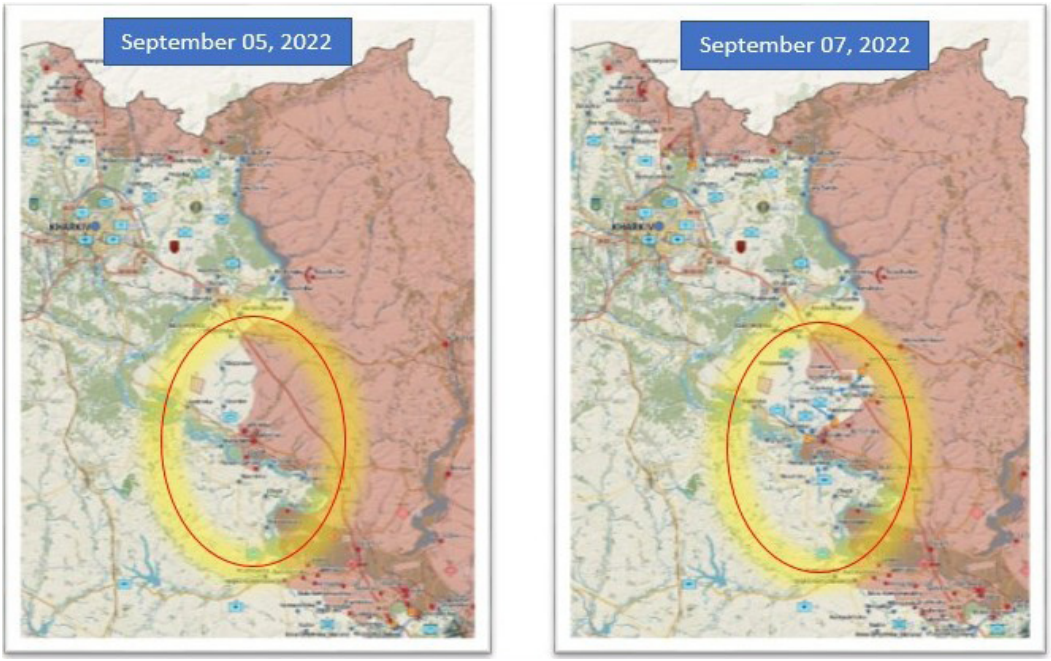


Figure no 2: Force disposition in Kharkiev region (Kharkiv Front 2024)

Feint. The Ukrainians have conducted multiple attacks in the southern area to create the illusion of a major offensive as it can be noticed in Figure no. 3 that depicts offensive operations conducted by the Ukrainians in Kherson area.

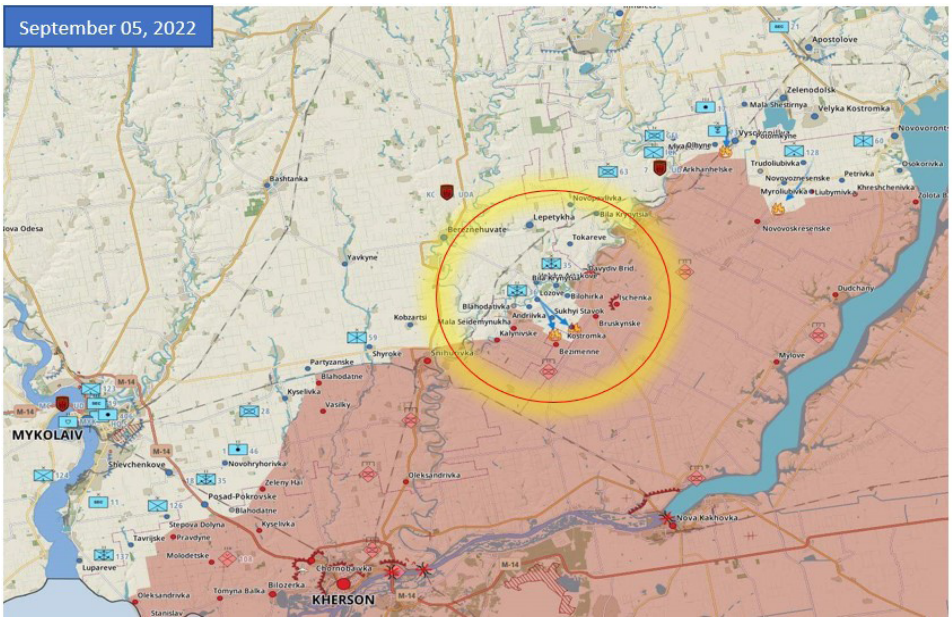


Figure no. 3: Feint attacks in Kherson area (Kherson Front 2024)

Disinformation. Disinformation has played a significant role in shaping Russian perception with respect to the location of the counteroffensive. In this respect, media has been used to reinforce enemy's perception on the false attack.

Camouflage. Ukraine has kept a low profile for the accumulation of forces in Kharkiv area in order to make the Russians believe that there are no imminent Ukrainians attacks in this area.

Denial. Denning Russians reconnaissance ability to collect relevant information that might have disclose real intentions of the Ukrainians through counter-reconnaissance missions as previously presented.

Furthermore, Ukrainian forces have made use of two main deception techniques. The obvious solution, making the Russians believe that Kherson will be the next logical move and then reinforcing that perception regarding the location of the counteroffensive. In the same time, Ukrainians have taken measures to suppress the signature of their force's accumulation in the north-east front, thus contributing to surprising the Russians on September 6, the beginning of the real offensive.

Moreover, it is worth noting that various channels of communication, such as media outlets and diplomatic channels, have played a significant role in shaping Russians' response to the deceptive observables that have been portrayed in Kherson. These platforms have proven to be instrumental in disseminating information and influencing their perception. While it is undeniable that Russian intelligence collection assets have served as a pivotal channel in this regard, it is important to acknowledge that the analysis at hand solely relies on open-source information, thus we cannot provide concrete evidence regarding their usage.

Feedback, one of the key principles of deception, was critical to the incremental success of the operation. Based on the indicators that we have highlighted in Table no 1, the Ukrainians had the opportunity to assess the progress of their operation, adapt it and optimize it in order to create the desired perception for the Russians and achieve the deception objectives. In this way, they made the story as credible, consistent, verifiable and executable as possible, which is actually another important principle of deception. Reinforcing the enemy beliefs through exploitation of their confirmation bias, also represented a key component of the Ukrainian deception plan.

Conclusions

Since ancient times, deception has been a vital component of military strategy, and its value cannot be overstated. The 2022 Kharkiv counteroffensive was no exception. This operation shows how important deceptive tactics can be to military strategy even today, as modern technology continues to advance. The use of disinformation and feigned movements allowed the Ukrainian forces to gain a strategic advantage. Furthermore, this operation demonstrated that modern

transparent battlefield is an illusion. Exploiting the fog of war, but also the enemy's preconceptions can significantly contribute to the success of military operations. Deception, as demonstrated again by the Ukrainians in the recent Kursk intervention is as relevant as ever. As such, it must be carefully studied and understood in order to be effectively employed by military forces.

The current study has done just that, offering a theoretical framework of deception analysis in the context of the 2022 Kharkiv counteroffensive. The analysis was focused on identifying key concepts specific to deception operation and reconstruct the Ukrainians approach on the counteroffensive. The value of this work lies in its potential to inform future military strategists and tacticians. Furthermore, the study might offer insights into the psychological aspects of deception in modern warfare and emphasize the importance of maintaining the element of surprise. Additionally, the paper highlighted the importance of media as a key channel of deception in the current operating environment, in addition to disinformation as a critical tactic of deception.

In conclusion, the 2022 Kharkiv counteroffensive demonstrated that deception is as viable today as it was more than 2000 years ago, when Sun Tzu stated that all warfare is based on deception, surprise still being possible in this "transparent battlefield".

BIBLIOGRAPHY:

AFM. 2018. *Army Field Manual - Warfighting Tactics Part 1: The Fundamentals.* UK Ministry of Defence.

2020. *AJP-2 Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security.* B, version 1. NATO Standardization Office.

Axe, David. 2022. *Russian Troops are Dashing around Ukraine Trying to Block Ukrainian Counterattacks.* September 08. Accessed August 27, 2024. https://www.forbes.com/sites/davidaxe/2022/09/08/russian-troops-are-dashing-around-ukraine-trying-to-block-ukrainian-counterattacks/

—. 2022. *The Bridge Battle In Southern Ukraine Is Escalating.* July 31. Accessed August 26, 2024. https://www.forbes.com/sites/davidaxe/2022/07/31/the-bridge-battle-in-southern-ukraine-is-escalating/

Bouwmeester, Han. 2021. "The art of deception revisited." *Militair Spectator* 190 (9): 420-434. https://www.militairespectator.nl/sites/default/files/teksten/bestanden/militaire_spectator_9_2021_bouwmeester.pdf

David Petraeus, Andrew Roberts. 2023. *Conflict. The evolution of Warfare from 1945 to Ukraine.* Harper Collins Publishers.

Dmytro Kruhliak, Danilo Komarov. 2023. "Counteroffensive operation of the Armed Forces of Ukraine on the Kharkiv direction in 2022: experience and strategic significance." *Bulletin of Taras Shevchenko National University of Kyiv History* (Taras Shevchenko National University of Kyiv) 157: 38-44.

Franz-Stefan Gady, Michael Kofman. 2024. "Making Attrition Work: A Viable Theory of Victory for Ukraine." *Survival* 66 (1): 7–24.

Freedman, Lawrence. 2022. *Gradually, then Suddenly.* September 10. Accessed August 26, 2024. https://samf.substack.com/p/gradually-then-suddenly

Friedman, B.A. 2017. *On Tactics. A theory of victory in battle.* Annapolis: Naval Institute Press.

George-Ion TOROI, Cristian-Octavian STANCIU. 2023. "PLANNING DECEPTION AT THE OPERATIONAL LEVEL OF WAR." *Romanian Military Thinking* 12-35.

2022. *In the Kherson direction began "very powerful" movement of Russian troops - Danilov.* July 27. Accessed August 26, 2024. https://www.radiosvoboda.org/a/news-khersonskyy-napryam-viyska-rf-danilov/31962539.html

IONIȚĂ, Crăișor-Constantin. 2023. *Convențional și hibrid în primul an al războiului Federației Ruse împotriva Ucrainei - Concluzii și lecții desprinse din război : studiu de specialitate.* Information, București: "Carol I" National Defence University Publishing House.

Isabelle Khurshudyan, Paul Sonne, Serhiy Morgunov, Kamila Hrabchuk. 2022. *Inside the Ukrainian counteroffensive that shocked Putin and reshaped the war.* December 29. Accessed August 27, 2024. https://www.washingtonpost.com/world/2022/12/29/ukraine-offensive-kharkiv-kherson-donetsk/

Jack Watling, Nick Reynolds. 2022. *Operation Z. The Death Throes of an Imperial Delusion.* Royal United Services Institute for Defence and Security Studies.

Jack Watling, Oleksandr V Danylyuk, Nick Reynolds. 2024. *Preliminary Lessons from Ukraine's Offensive Operations, 2022–23.* London: Royal United Services Institute.

2024. *Kharkiv Front.* Accessed August 28, 2024. https://militaryland.net/maps/russian-invasion/kharkiv-front/

Kharuk, Andrii. 2023. "Slobozhan offensive operation: prerequisites and the first stage (September, 6—12, 2022)." *Ukrainian Historical Journal* 1: 5-19.

2024. *Kherson Front.* Accessed August 28, 2024. https://militaryland.net/maps/russian-invasion/kherson-front/

Koffman, Michael. 2024. "The Russian-Ukraine War. Military Operations and Battlefield Dynamics." In *War in Ukraine : conflict, strategy, and the return of a fractured world*, by Hal Brands, 99-120. Baltimore, Maryland: Johns Hopkins University Press.

Lyndon Benke, Michael Papasimeon, Tim Miller. 2021. "Modelling Strategic Deceptive Planning in Adversarial Multi-Agent Systems." *Deceptive AI: First International Workshop, DeceptECAI 2020, Santiago de Compostela, Spain, August 30, 2020 and Second International Workshop, DeceptAI 2021, Montreal, Canada, August 19, 2021, Proceedings 1* 76-83.

Michael Bennett, Edward Waltz. 2007. *Counterdeception Principles and Applications for National Security.* London: Artech House.

Mykhaylo Zabrodskyi, Jack Watling, Oleksandr V Danylyuk, Nick Reynolds. 2022. *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022.* Information, London: Royal United Services Institute for Defence and Security Studies.

Nagl, John A. 2024. *A call to arms: Lessons from Ukraine for the Future Force.* Strategic Studies Institute, UIS Army War College.

Nathan Hodge, Daria Markina, Tim Lister, Niamh Kennedy, Lindsay Isaac. 2022. *Russia says it will reduce military operations around Kyiv following talks with Ukraine.* March 22. Accessed August 26, 2024. https://edition.cnn.com/2022/03/29/europe/russia-reduce-assault-kyiv-plan-intl/index.html

2018. *Planning and Execution Handbook.* UK Ministry of Defence.

Plokhy, Serhii. 2023. *The Russo-Ukrainian War. The return of history.* New York: W. W. Norton & Company.

Ponomarenko, Illia. 2022. *What would a Ukrainian counter-offensive in Kherson look like?* July 19. Accessed August 27, 2024. https://kyivindependent.com/what-would-a-ukrainian-counter-offensive-in-kherson-look-like/

Porter, Tom. 2022. *Ukraine celebrates US long-range rocket systems arriving after months of asking. 'Summer will be hot for Russian occupiers.'.* june 23. Accessed August 26, 2024. https://www.businessinsider.com/ukraine-hails-arrival-himars-predicts-pain-for-russia-2022-6

2022. *President of Ukraine.* August 29. Accessed August 26, 2024. https://www.president.gov.ua/en/news/okupanti-mayut-znati-mi-gnatimemo-yih-do-nashogo-kordonu-lin-77413

Robert M. Clark, William L. Mitchell. 2019. *Deception: Counterdeception and Counterintelligence.* Los Angeles: CQ Press.

2022. *Russia's War in Ukraine: Military and Intelligence Aspects.* Informal, Washington DC: US Congresional Research .

2022. *Russian Offensive Campaign Assessment, August 1.* August 01. Accessed August 27, 2024. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-august-1

2022. *Russian Offensive Campaign Assessment, August 11.* August 11. Accessed August 27, 2024. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-august-11

2022. *Russian Offensive Campaign Assessment, August 2.* August 02. Accessed August 27, 2024. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-august-2

2022. *Russian Offensive Campaign Assessment, August 20.* August 20. Accessed August 27, 2024. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-august-20

2022. *Russian Offensive Campaign Assessment, August 24.* August 24. Accessed August 27, 2024. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-august-24

2022. *Russian Offensive Campaign Assessment, August 9.* August 09. Accessed August 27, 2024. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-august-9

2022. *Russian Offensive Campaign Assessment, July 12.* July 12. Accessed August 27, 2024. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-july-12

2022. *Russian Offensive Campaign Assessment, July 13.* July 13. Accessed August 27, 2024. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-july-13

2022. *Russian Offensive Campaign Assessment, July 19.* July 19. Accessed August 27, 2024. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-july-19

2022. *Russian Offensive Campaign Assessment, July 30.* July 30. Accessed August 27, 2024. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-july-30

2022. *Russian Offensive Campaign Assessment, September 4.* September 04. Accessed August 27, 2024. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-september-4

2022. *Russian Offensive Campaign Assessment, September 6.* September 06. Accessed August 26, 2024. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-september-6

2023. *Russian War Against Ukraine. Lessons Learned Curriculum Guide.* Bruxelles: NATO Headquarters.

Ryan, Mick. 2022. *A tale of three generals — how the Ukrainian military turned the tide.* October 14. Accessed August 24, 2024. https://engelsbergideas.com/essays/a-tale-of-two-generals-how-the-ukrainian-military-turned-the-tide/

Seth G. Jones, Jake Harrington, Christopher K. Reid, Matthew Stohmeyer. 2023. *Combined Arms Warfare and Unmanned Aircraft Systems. A new era of strategic competition.* Washington DC: Center for Strategic and International Studies.

Shandra, Alya. 2022. *'Ukraine's counteroffensive near Kharkiv: what enabled the Balakliia blitzkrieg.* September 11. Accessed August 24, 2024. https://euromaidanpress.com/2022/09/11/ukraines-counteroffensive-near-kharkiv-what-made-the-blitzkrieg-possible/

2022. *Shoigu announced the attempts of the APU to the Nikolaev-Kryvorozhsky and other directions.* September 02. Accessed August 26, 2024. https://www.interfax.ru/world/860425

Strachan, Hew. 2022. *The art and science of intelligence in war.* August 15. Accessed August 26, 2024. https://engelsbergideas.com/essays/the-art-and-science-of-intelligence-in-war/

Trevelyan, Mark. 2022. *Russia declares expanded war goals beyond Ukraine's Donbas.* July 20. Accessed August 26, 2924. https://www.reuters.com/world/europe/lavrov-says-russias-objectives-ukraine-now-go-beyond-donbas-2022-07-20/

Trofimov, Yaroslav. 2024. *Our enemy will vanish. The Russian invasion and the Ukraine's war of independence.* New York: Penguin Press.

2002. *Ukraine claims responsibility for Crimea attacks.* September 07. Accessed August 26, 2024. https://www.aljazeera.com/news/2022/9/7/ukraine-military-chief-claims-responsibility-for-strikes-in-crime

2022. *Ukraine Strategy Targets Russian Army's Lifelines in Kherson.* August 17. Accessed August 26, 2024. https://www.bloomberg.com/news/articles/2022-08-17/ukraine-strategy-targets-russian-army-s-lifelines-in-kherson?embedded-checkout=true

2022. *Ukraine's southern offensive 'was designed to trick Russia'.* September 22. Accessed August 26, 2024. https://www.theguardian.com/world/2022/sep/10/ukraines-publicised-southern-offensive-was-disinformation-campaign

2022. *Ukrainian adviser warns progress will be slow as southern counterattack begins.* August 29. Accessed August 26, 2024. https://www.theguardian.com/world/2022/aug/30/zelenskiy-tells-russian-forces-to-flee-as-ukraine-counteroffensive-begins-in-kherson

2022. *Ukrainian forces in Kharkiv reach Russian border.* May 16. Accessed August 26, 2024. https://www.dw.com/en/ukraine-forces-in-kharkiv-push-through-to-russian-border-as-it-happened/a-61808824

2022. *Video from Antonivka Road Bridge in Kherson shows extensive damage.* July 27. Accessed August 26, 2024. https://www.yahoo.com/video/video-antonivka-road-bridge-kherson-081127402.html?guccounter=1

2022. *Zelensky ordered to reconqual the south of Ukraine - Reznikov.* July 11. Accessed August 27, 2024. https://www.dw.com/uk/zelenskyi-nakazav-vidvoiuvaty-pivden-ukrainy-reznikov/a-62432972

DOI: 10.53477/1842-9904-24-8

TRANSATLANTIC PARTNERSHIP – POLITICAL DEVELOPMENTS AND TRANSFORMATIONS IN THE NEW GEOSTRATEGIC FRAMEWORK

Ilinca-Smaranda CIOATĂ*

Considering a series of events from the last ten years, politically and militarily relevant, International Relations scholars are questioning the robustness of the Euro-Atlantic relations. However, such a cooperation, that started decades ago, does not end without serious consequences that can go beyond the area of the involved parties. The main assumption of this article is that, for the short term, no serious transformation – such as a division between the European and the American parties, be it political, military, or economic – can take place in the present security framework – without severe implications for the global order. However, in the longer term, the cooperation can find a rather independent European Union – thought not entirely, capable of defending itself and projecting its military power beyond its borders (European Parliament 2022, 1). For the purpose of this article, there will be analysed the relationship between the European Union and NATO, based on the latest strategic documents adopted in 2022 by the two organizations – EU's Strategic Compass and NATO's Strategic Concept, as well as the most recent Joint Declaration signed by the two partners in January 2023. The latter provides common responses to new challenges and joint efforts to promote an international environment based on stability and prosperity, and the condemnation of the actors who cause instability affecting peace and security. The overall objective is to present the ability of the two organisations to adapt to the new challenges and threats in order to achieve their common objectives. The expected outcome of the analysis is to position the Transatlantic Partnership as a fundamental element of stability in the transatlantic area through the implementation of agreed security and defence strategies and objectives.

Keywords: *European Union (EU); The North Atlantic Treaty Organization (NATO); cooperation; partnership; security; defence; crisis management.*

**** Ilinca-Smaranda CIOATĂ is a PhD Student in the field of Political Science University "Alexandru Ioan Cuza", Iași, România. E-mail: ilinca.cioata@gmail.com***

Introduction

The European Union (EU) works together with the North Atlantic Treaty Organization (NATO) to prevent and resolve crises and conflicts in the Euro-Atlantic area. Sharing common interests and strategies, the two organizations cooperate on the basis of the principles of complementarity and partnership. Joint efforts to combat security challenges are key priorities set out in jointly adopted documents and strategies. Collaboration in different areas of common interest between NATO and the EU is therefore an important element of a comprehensive approach to international crisis and conflict management, drawing on both civilian and military means.

NATO-EU cooperation is, in fact, an essential pillar for strengthening security and defence in the transatlantic area, at the same time contributing to global stability. A strong European Union is complementary to a strong NATO and therefore mutually reinforcing.

Cooperation between NATO and the EU has been strengthened by the most recent Joint Declaration signed on 10 January 2023 in Brussels. The document sets out the common vision of how NATO and the European Union will act against challenges and threats to Euro-Atlantic security. In brief, the two organizations will intensify their collaboration in areas such as growing geostrategic competition, resilience issues, protection of critical infrastructures, emerging and disruptive technologies, space, security implications of climate change, foreign information manipulation and interference (European Council 2024).

Therefore, the Partnership was created as an expression of the shared principles that stability and security in the transatlantic area can only be achieved through cooperation and joint action. Promoting human rights and freedoms, peace and security are some of the Partnership's fundamental shared values. Both NATO and the EU will continue to cooperate in the future, as they are aware that only together they can have a unified voice on issues arising from the dynamics of the geostrategic environment. Moreover, sharing the same values and strategic interests provides a basis for partnership.

1. Crisis Management from NATO and EU Perspective

In contemporary international relations, crises and conflicts are becoming more complex. Both states and international organisations are actors involved in the process of conflict and crisis management and their main goal is to ensure peace and security. For the international relations field, crisis management and conflict solution is a relatively recent field, having developed since the Cuban Missile Crisis of 1962.

In academia, crisis is defined as "a change in the course of an event, activity or relationship due to a complex of causes from economic to psychological" (Duțu 2013, 9). In practice, crises and conflicts are realities, in fact situations that the international environment will always face. Preventing and anticipating them requires, first, knowledge and study, and an appropriate strategy to manage them effectively. In this respect, crisis and conflict management plays the most important role. In fact, crisis management involves a set of measures and actions aimed at stopping the evolution of a crisis into a violent course, or to stop the escalation of aggressions into an armed conflict. The response of actors involved in crisis management must be prompt, the goal being to prevent escalation into armed conflict whether intra- or inter-state. Crisis management has developed gradually by using civilian and military capabilities in crises before they turn into armed conflicts, but especially by enhancing security and stability in post-conflict situations.

Sharing the same strategic interests and principles and facing similar challenges and threats, NATO and the European Union have decided to join forces in cooperating on issues of common interest, becoming increasingly involved in crisis management and international conflict resolution. In order to understand the role played by the two organisations in crisis management, we will try to briefly highlight the perception of security threats and challenges, by analysing the strategies adopted in recent times.

Crisis management manifests itself differently depending on the nature of the organisation involved. As a military-political organisation, NATO uses both military and civilian instruments to solve international crises. For NATO, crisis management has been a constant concern and has been on the agenda since the organisation's formation under the Washington Treaty signed in 1949. In the Treaty, we find in Article 4 and Article 5 concepts such as *joint consultations*, *attack against all*. There are three phases in NATO's strategic thinking on crisis management: the Cold War phase, the period after the end of the ideological confrontation between East and West, and the period after the attacks of 11 September 2001. Crisis management at NATO level is defined as those coordinated actions taken with the aim of defusing crises, preventing their escalation into armed conflict and at the same time limiting hostilities if they should result (Groșeanu 2013, 13).

Over time, more precisely after the end of the ideological confrontation between the US and the USSR, NATO, through the Strategic Concepts adopted, tried to adapt to the new security environment by developing a Non-Article 5 dimension to crisis management. This dimension also refers to situations where conflicts erupt outside the transatlantic area and the aggression does not directly target a NATO member state, "when these have the potential to affect Allied security" (NATO 2022, art. 35). Therefore, each Strategic Concept has developed the crisis management concept at NATO level, but the purpose remains unchanged, that is to prevent international conflicts and crises through a controlled response (D. Ghiba 2014, 51).

The Alliance's vision of crisis management changes considerably with the adoption of *The 1999 Strategic Concept*. According to this new document, crisis management is much more clearly defined and included in the main tasks of the organisation. The Alliance's fundamental tasks are security through cooperation, consultation, and dissuasion and defence. In practical terms, the concept includes for the first time the possibility of consultation/cooperation between NATO member states and other international actors, such as the European Union. With this NATO concept, it is also decided to strengthen relations with the European Union, an aspect that is pursued in every strategy adopted subsequently.

Crisis management takes on a new form with the adoption of the 2010 Lisbon Strategic Concept. The signing of the new concept was triggered simultaneously by the process of reforming and transforming NATO, its command and control structure, resources, etc., while strengthening the Alliance's role in the international system with new capabilities and new partners. In view of the new challenges to the transatlantic security environment (migration, terrorism, inter-ethnic conflicts, etc.), greater emphasis is being placed on crisis management as one of the Alliance's core tasks, thus moving from being an instrument for ensuring international stability and peace to an end in itself. Thus, international crisis and conflict prevention and post-conflict reconstruction are NATO priorities achieved mainly through cooperation among Allies, as well as with external partners such as the EU, engaging when the circumstances demand it.

Responding to the threats and vulnerabilities of the international security environment, in 2022 NATO decided that it was time for new internal reforms, and the Madrid Summit reaffirmed the Alliance's main purpose of ensuring collective security by resorting this time to a 360-degree posture: "We will employ military and non-military tools in a proportionate, coherent and integrated way to respond to all threats to our security in the manner, timing and in the domain of our choosing" (NATO 2022, 6).

Regarding to crisis management, the Alliance expresses its desire to improve the effectiveness of the crisis response system by stepping up planning activities and thus continuing to "work to prevent and respond to crises when these have the potential to affect Allied security", and to "invest in crisis response, preparedness and management, through regular exercises and leverage our ability to coordinate, conduct sustain and support multinational crisis response operations" (NATO 2022, 9).

Crisis management has become the Alliance's only operational mechanism for maintaining and promoting stability in the Euro-Atlantic area, comprising two strands of action: conflict prevention and Crisis Response operations. Crisis management operations in which NATO is involved "are centred on the use of military force to resolve a conflict or crisis involving actors outside its borders" (Bogzeanu 2011, 7-10). In other words, NATO is an organisation with a strong military character,

which, of course, also defines the approach to crisis management in which it is involved. NATO has the capability to undertake a wide range of military operations and missions including peacekeeping operations, peace-making, conflict prevention, disaster relief operations and missions in response to natural disasters, maritime security missions, air policing missions (NATO 2023). The accent on the hard power is predominantly felt in every mission in which NATO engages.

Compared to NATO, which is a military-political organisation, the approach to the concept of crisis management in the European Union is a slightly different. Being a political and economic organisation, the security and defence dimension has developed recently, in the context of the failed management of the Western Balkans crisis that led to the break-up of Yugoslavia in the 1990s. The Union's particularity in terms of crisis and conflict management consists in the common effort to increase CFSP/CSDP coherence in such a way as to allow it, through the mechanisms and instruments adopted, to perform missions and operations in the international arena. Even if the European Union has not developed a crisis management framework as consistent and coherent as NATO, this does not mean that it does not have a strong voice in this area. The continued development of the CSDP denotes the Union's efforts to become an important and influential strategic actor at global level. The missions and operations in which the EU engages intensify its role in the field of crisis management and conflict resolution.

The European Union does not offer a precise and clear conceptualisation of the term crisis management. It takes to the form of an integrated mechanism that allows the Union to intervene in major and complex crises situations with the intention of preventing an escalation of the crises and with the aim to deliver aid and resolve the situation. Another explanation of the term can be summarised as - a set of all non-military/military instruments and EU policies that are mainly used in crisis management process according to CSDP and the strategies adopted at the level of the Union (European Council 2024). Moreover, for accomplishing its operations, the EU relies on NATO capabilities, according to the "Berlin Plus" arrangements.

The European Union's crisis management efforts in recent years have been crystallised in the formation of the following mechanisms (European Peace Facility, EU Rapid Development Capability, Crisis Response Coordination Centre) that respond to the new challenges of the 21st century, while ensuring that it can intervene to deliver aid. For example, European Peace Facility (EPF) was created at the initiative of the HR/VP Federica Mogherini with the support of the European Commission. In essence, the EPF is a European off-budget tool that helps "enhancing the Union's ability to prevent conflicts, build peace and strengthen international security, by enabling the financing of operational actions under the Common Foreign and Security Policy (CFSP) that have military or defence implications" (Federal Ministry of Defence of the Republic of Austria 2021, 103).Thus, the EPF aims to

develop the application sector of common costs by financing essential capacities for EU operations and missions. As for the EU Rapid Deployment Capacity (EU RDC), it was established by the proposal of the HR/VP Josep Borrell, one of the main military outcomes of the Strategic Compass of the European Union. The EU RDC will improve the EU's ability to react effectively in crisis situations, and will allow to swiftly deploy a modular force of up to 5000 troops, including land, air and maritime components, as well as strategic enablers (European Union External Action 2023). Last but not least, Crisis Response Coordination Centre (ERCC) was launched in 2013 with the objective of providing aid to countries affected by disasters. The ERCC is considered the heart of the EU Civil Protection Mechanism and "acts as a coordination hub between all EU Member States, the 10 additional participating states, the affected country, and civil protection and humanitarian experts" (European Commision 2023). In crisis situations, rapid and coordinated response is vital to save lives and minimize damage. This is where the EU ERCC comes into play.

The Union's approach to crisis management is closely connected to its strategic partnership with NATO: its cooperation with the North Atlantic Alliance, has contributed significantly over the years both to the development of the security and defence dimension at Union level and to the conduct of EU-led missions using Alliance capabilities and resources under the provisions of the "Berlin Plus" agreements (Ghiba and Pleșanu 2018, 88). The difference between the two organizations is seen in the way they engage in crisis situations. More specifically, the EU authorities approach crisis management from a non-military perspective, using peaceful and civilian means, a strategy which gives it a special status in the field of international relations. The approach is also different from the point that this whole crisis management process takes place within the framework of the Common Foreign and Security Policy. This means that any intervention, whether military or civilian, can be influenced by the fact that the Member States' interests must also be taken into account, which makes it difficult to create a united, common and coherent vision (Ghiba and Pleșanu 2018, 89). Moreover, the EU has a different approach regarding two important security concepts, namely *conflict prevention*, which includes activities carried out before a crisis escalates into hostile action, and *crisis management*, which involves intervention after violent action. The process of post-conflict reconstruction is understood at European level as a means of preventing the outbreak of a future crisis.

In the case of the European Union, missions deployed using civilian capabilities – humanitarian aid, post-conflict reconstruction, development aid, etc. –give it a different voice in international crisis management. The crisis management missions and operations conducted by the Union on three continents, of which nine are currently military (such as *EUMAM* - Ukraine, Central African Republic - *EUTM*

CAR, Operation Sophia - *EUNAVFOR MED*, Somalia - *EU NAVFOR)*, and 12 civilian (among which Georgia - *EUMM,* Iraq - *EUAM*, Kosovo - *EULEX*, Libya - *EUBAM*, Mali - *EUCAP SAHEL*) show that the Union is prepared to take risks for peace and responsibilities in international security (European Union External Action 2023). The greater focus on the civilian component of crisis management is determined both by the absence of a permanent European command and control structure and by the budget allocated to this area. For example, civilian missions are financed from the EU budget, while military operations are supported from the national budget of the state/states that decide to take part in the mission (85%-95% national funding, 5%-15% European funding, on the basis of Athena mechanism) (Curtea de Conturi Europeană 2019, 23-24).

Although the European authorities have developed more the civilian side of crisis management and less the military one, there is nevertheless a mutual clause in the Lisbon Treaty between Member States allowing them to act militarily. The mutual assistance clause in Article 42 (7) of the Treaty states that if a Member State is the victim of armed aggression on its territory, the other Member States shall be obliged to provide aid and assistance by all the means in their power, in accordance with Article 51 of the Charter of the United Nations (EUR-Lex 2023). This clause has not been used since 2015. This may raise many questions about the unity and vision of the European Union, especially in the context of an armed conflict on the eastern border, which inevitably affects security and stability within the European Union. For example, in the case of Ukraine, the European Union has been put in the position of acting on the principle of unity in terms of economic and military aid, but especially in terms of accession to the EU. This has sparked disputes and contradictions between Member States. Hungary's adverse offensive position in this case is well known. Even more, the Member States are vigilant to this case, as the presidency of the EU Council has been taken over by Hungary in the second semester of 2024.

The last few years are proof that the European Union has made efforts through the strategies adopted (Global Strategy in 2016 and the Strategic Compass in 2022) to reform the Common Foreign and Security Policy, including the Common Security and Defence Policy, in order to guarantee its status as a strong international power. Under these circumstances, the EU is increasingly becoming a global player, which is also involved in resolving international crises, with the aim of maintaining international peace and security. This new role that the Union wants to take on needs to be much more clearly defined, and when it decides to engage in conflict resolution, it needs to take a firm position, a point also made in the strategy paper adopted in March 2022: "We have to be bolder in how we combine our diplomatic and economic instruments, including our sanctions regimes, with civil and military assets to prevent conflict, respond to crises, contribute to peacebuilding and support partners. We will

also strengthen our cooperation with bilateral, regional and multilateral European security and defence initiatives that contribute to Europe's security" (Council of the European Union 2022, 12). Only under these conditions can the European Union assume its role as a stabilizing factor in Europe and beyond.

The different nature promoted by NATO and the EU on security and defence issues inevitably leads to complementary views that can essentially facilitate a comprehensive approach to security in terms of its military and civilian dimensions.

2. Strengthening the Partnership

The time of instability in the Euro-Atlantic area caused by the conflict between the Russian Federation and Ukraine has pushed NATO and EU partners to take the initiative to adopt new strategies to respond to common threats and challenges in a united way.

The adoption in 2022 of the EU's Strategic Compass and NATO's Strategic Concept gave a new impulse to the transatlantic partnership, confirming the importance of strategic unity. Both documents highlight the need for closer transatlantic cooperation on common security threats: "The EU and NATO remain firmly committed to further strengthen, deepen and expand their mutually reinforcing and beneficial cooperation by exploring avenues for further collaboration across all existing work strands, as well as in new areas such as climate and defence, space and emerging and disruptive technologies, in full respect of the agreed guiding principles (mutual openness and transparency, inclusiveness and reciprocity, and decision-making autonomy of both organisations)" (European Council 2024).

In the context of Russia's military aggression against Ukraine, the transatlantic partnership is more than essential. As highlighted in both NATO and EU strategic documents, the international environment is at a critical moment affecting Euro-Atlantic security and stability, demonstrating the importance of the transatlantic partnership. Only through a strong and closer cooperation can security and stability be maintained within the organisations.

The transatlantic partnership is stronger and more relevant than ever, and political dialogue, intelligence sharing, military mobility and the development of military capabilities are actions taken by the two organisations in recent times. Constantly adapting to the threats and challenges that arise in the security environment is the prompt and effective response provided by NATO and the European Union.

In the Strategic Compass it is underlined the need to strengthen cooperation with NATO in order to be able to meet new security threats and challenges. Strengthening the strategic partnership with NATO goes hand in hand with the strengthening of CSDP civilian and military missions through which the Union can provide a more rapid and comprehensive response in crisis management: "We need to be able to act

quickly and robustly whenever a crisis erupts, with partners if possible and alone when necessary" (Council of the European Union 2022, 3). The Strategic Concept actually complements the EU position and vision on common threats. NATO and the EU thus have complementary and coherent roles in preserving international peace and security.

As a unique and essential partner for the Alliance, the European Union is developing civilian and military capabilities that strengthen its security and defence role. A stronger and more capable Union strengthens the transatlantic partnership and also contributes to stability in the area: "NATO recognises the value of a stronger and more capable European defence that contributes positively to transatlantic and global security and is complementary to, and interoperable with NATO" (NATO 2022, 10).

Periodic meetings between NATO and the EU are aimed at improving political dialogue, and with it the exchange of classified and unclassified information. A common awareness of situations and factors affecting the stability of the transatlantic area and constant adaptation to the current security environment enhances EU-NATO collaboration and cooperation at the highest level. In order to improve the political dialogue, the transatlantic partners should organize more frequent and inclusive joint meetings, focusing on strategically relevant issues (Council of the European Union 2022, 39). Moreover, the full involvement of non-EU Allies in the development of the security and defence component of the Union is essential to strengthen the NATO-EU partnership, and joint exercises would enhance NATO-EU cooperation at all levels, while strengthening mutual confidence. This would allow for a strengthening of the partnership through an appropriate exchange of information leading to improved NATO-EU interoperability. The key to improving transatlantic cooperation lies in the strength and capacity of both partners to constantly adapt to new international security challenges and threats. Joint efforts to secure the Euro-Atlantic area must therefore also include an increase in defence spending, thereby improving existing capabilities while avoiding unnecessary duplication.

Thus, starting with 2023, the NATO-EU partnership has moved to a new phase of evolution and political dialogue and cooperation will be the instruments used in all areas of interaction, from resilience, technologies, climate, to defence and security.

3. Strategic Challenges and Limitations

Cooperation between the two organisations can be traced back in the 1990s. This cooperation has taken the shape of a natural relation between the actors who share the same goal: achieving and maintaining security, stability, and prosperity. Thus, the efforts made by the two international actors, in the field of security and

defence, have been contributing to the stability and security of the Euro-Atlantic area. It can hardly be argued that Europe and North America would look the same without this strong transatlantic connection.

Starting as a traditional relationship based on diplomatic exchanges, shared values and common interests, transatlantic relations have gradually evolved into a continuing relationship of cooperation on security and defence. However, there are also areas (such as funding, namely the percentage allocated by Member States who takes the lead of a future mission) that generate strong contradictions in the partnership, threatening the cohesion of the EU-NATO relationship, turning it from a state of cooperation into a state of competition.

The high-level cooperation between the two organizations has certainly also influenced the way they relate and approach to the challenges, threats and risks of the security environment. Once the partnership is created, it is understood that the challenges and threats faced by the EU (terrorism, organized crime, corruption, inter-state conflicts, and cybersecurity) are equally threats and challenges to NATO and vice versa. That is why cooperation must cover as many areas of common interest as possible and aim at a single goal: creating a stable transatlantic environment for the long term. Moreover, the similar perception of the international security environment also implies a complementary approach by the two partners. Due to the duplication of Member States (a major part of the EU Member States are also part of NATO) security and defence interests often overlap, which seems to limit the partnership. Continuing on this note, we can state that one of the greatest strategic limitations of the partnership is closely linked to the cooperation and collaboration between the US and the EU. Depending on the interests and policies adopted by Washington, the EU-NATO relationship is either cooperative or competitive (Joja, Iulia-Sabina 2021). Donald Trump's coming to power implies, among other things, a change in the approach to transatlantic cooperation. The policy adopted by the Republican President has inevitably diminished the credibility of the EU Member States in the American guarantee and NATO alike. Trump's unpredictable policy has contributed to deepening already existing divergences within the partnership, generating new ones, in terms of defence spending and the percentage allocated by European allies (Sloan 2021, 8). Despite the policy pursued by Trump, relations between the partners started to return to normal with the change of the US administration with the election of Joe Biden in 2021. His pro-European speech gave the EU a new security and defence guarantee.

Looking at these aspects, we can easily see a major risk in EU-NATO relations. When transatlantic relations are on an ascendant trend (as in the case of the Biden administration), cooperation among EU Member States on security and defence is strained, while when the divergences in the partnership are increasingly accentuated (in the case of the Trump administration), the EU focuses on developing its own

strategies to ensure its security and defence interests – developing CSDP and its instruments, as for instance when elaborating and adopting the Strategic Compass (Romanyshyn 2021, 1).

Relaxation of the EU risks compromising, to a greater or lesser extent, the process of developing its own strategic mechanism, which would inevitably also lead to a weakening of the preconditions for a more balanced and effective transatlantic link. In the context of the new security challenges – Russia's war of aggression against Ukraine, the conflict situation in the Middle East – this risk becomes even more pronounced, and the decision by the EU to allocate a smaller budget to security and defence may have far deeper implications.

Many times the question arises whether NATO defence is enough, or should the European Union be more active in the field of security and defence? Perhaps one of the most common answers would be that NATO would be sufficient to provide security for both the transatlantic area and even for the world. However, we should not forget that the best security and defence can be achieved collectively. Therefore, the fundamental principle of any collective defence organisation and beyond should be to combine the military and civilian power of its members in such a way as to discourage any potential attack against any ally (Ghincea 2017, actualizat 2022). In addition, to become an influential voice on security matters, the EU needs to overcome its military weakness, and create a fully operational armed instrument as a result of European defence cooperation efforts, even though Military Planning and Conduct Capability (MPCC) has been established since June 2017 (Council of the European Union 2019, 6). When it engages in operations and missions, it needs to take a firm stance to help end hostilities, not just to ease the situation.

To manage crises efficiently, the two organizations need, first and foremost, a common strategy, but above all joint action. To this end, the Union must increasingly develop its capacity for autonomous action, backed up by credible military and civilian forces and the necessary means. What is more, in order to have a concrete security response, I believe that the European Union needs to transform its security policy in such a way that it becomes more active and better connected to the threats and challenges generated by the current security environment. When deciding to intervene in certain conflicts, the EU has a rather palliative approach - it intervenes, often with ineffective methods that only seem to ameliorate differences and less to resolve the situation itself. A first look at the EU's intervention initially reveals an inability to react quickly due to both internal misunderstandings and the complexity of the decision-making process that underlies the launching of a mission. In addition, European missions should have a more scrutinized mandate, with clearly set and well-defined objectives from the outset that meet the needs on the ground. Therefore, the EU's security policy must be balanced and realistic in order to face current and future challenges and threats.

On the other hand, NATO should commit itself to addressing security threats and challenges by developing a strategy that emphasizes greater levels of deterrence against unconventional and hybrid attacks. The adoption of such a strategy should aim at a more targeted and efficient allocation of resources and instruments in such a way as to avoid the escalation of a conflict by using as little armed force as possible. In addition, consideration should be given to the development of additional complex defensive tools such as the simultaneous deployment of multiple defence systems, investments in anti-missile systems and the drone wall. Finally, the allies must realize that one of the most important deterrence methods is also the most feasible at this moment, namely the collective deployment of military training and capabilities in areas of greatest interest, such as the Eastern Flank and the Black Sea area. It is time for NATO to move to the next level and to realize the importance of developing a strategy for the Black Sea region as well, especially in the context of Russia's war against Ukraine. Strengthening regional and transatlantic security requires NATO to shape new goals, committing collective resources to help develop more coherent defence and deterrence systems. Such a strategy should pursue several fundamental objectives, namely: constantly improving the security environment of NATO members, but especially those in the Black Sea area; limiting Russian aggression against allies; and granting membership to those states that can guarantee the creation of a more secure environment for the transatlantic space (Joja, Iulia Sabina 2024).

Although the strategies of the two organizations cover issues related to security threats and challenges, there seems to be a lack of a specific chapter that defines the concrete way to manage and engage in crisis situations. The reality often differs greatly from the aspirations and objectives set by allies. The failure of NATO and the EU to induce Russia's renunciation of hostilities against Ukraine through the sanctions imposed raises many questions concerning the role of the two partners as a *stabilizing factor* in the transatlantic area and beyond.

There are some lessons that the West should learn from Russia's action against Ukraine, namely that history can repeat itself. So, how are allied states preparing to respond to a new threat from Russia? At the moment, we see more rhetoric and ultimatums, and less concrete actions. The European Union in particular must keep in mind that this conflict could essentially affect the entire European security architecture, given Russia's position vis-à-vis the ex-communist states. Future steps taken by the allies must include aspects of long-term investment in European security and the security of the Eastern flank of the partnership; increased investment in the security of strategic partners; strengthening strategic partnerships; and ad hoc consultations and dialogues with states of strategic interest (Joja, Iulia Sabina 2022). What the two partners can do is invest more in their partnership, especially those states that serve as bastions against Russian aggression. NATO and the EU must also

continue the *policy of containment* and not relax the sanctions imposed so far on Russia. Moreover, you cannot expect a state like Russia to stop its aggression against Ukraine as long as there is no unity in decision-making within the partnership, and moreover, within each of the two organisations. It is well known that Hungary has a different position on the war in Ukraine, but especially on the economic and military aid provided by NATO and the EU. Hungarian Prime Minister Orban has often declared that the aid provided to Ukraine only brings Europe, and therefore NATO, closer to a conflict with Russia, even though the intention is to prevent the escalation of Russian aggression and not to get involved in a war with Russia.

It is our belief that the transatlantic relationship needs to move to the next level in order to succeed in fulfilling the objectives set out in their joint declarations. This stage must take into account two essential directions: military mobility and defence capabilities, and security on the Black Sea. Military mobility is an absolute priority for the EU, NATO and their member states. Military mobility combines all activities undertaken for the rapid movement of armed forces and military equipment and beyond. Also, military mobility is an essential and credible action in the process of deterring a potential adversary taking military action, such as Russia (Chihaia 2024). When NATO and the EU include these two aspects as a fundamental priority in their strategies, then surely the partnership will move to another level. Moreover, the common voice will be heard globally, which would make crisis management much more effective than at present. As long as the constant development of the CSDP allowing the Union to become an influential security power is often understood as an attempt to weaken EU-NATO cooperation, things will remain at the same stage, more of trying and less of resolving crisis situations, as is the case in Ukraine. On the contrary, the assumption of a global role by the EU should be seen as complementarity and less in terms of competition, since the EU has developed its civilian component more. In reality, things are slightly different. In the ambitions for international domination, it is frequently overlooked that a joint force can have a stronger effect in restoring international order and security when needed. However, it seems that the NATO Summit in Washington in 2024 went in the same direction that we have become accustomed to so far – theoretical and conceptual deterrence, but with a different twist – the realization that transatlantic problems are not only external in nature, but also arise from internal vulnerabilities of member states' democracies (such as the rise of extremism). Things are not simple, and the current situation is reminiscent of entering a new era of the long war, in which it seems that NATO deterrence and the economic sanctions imposed by the EU are no longer sufficient or credible to stop the Kremlin's aggression. The continuation of the war is a wake-up call for the Occident that it is time to act, and why not, if attacked, to be ready to fight in the near future (Naumescu 2024).

Conclusions

Today's crises do not stop at the external borders of a state or region, moreover, they are becoming more complex and interconnected, with the effect often being felt globally. A good example of this is the COVID-19 pandemic, or the crisis generated by the war between Russia and Ukraine. In these circumstances, NATO needs a strong partner, and this can only be achieved by the European Union assuming a greater global role regarding defence. The Union must therefore increasingly strengthen its security and defence policy if it wants to succeed in meeting reasonable expectations as a credible and equal transatlantic partner able and willing to manage crises effectively, taking the lead when necessary but in close coordination with NATO.

The idea of developing a European pillar within the North Atlantic Alliance has been readily accepted and even encouraged by the Allies, and is known as the European Security and Defence Identity (ESDI). It was created with the aim of strengthening European participation in security matters while enhancing transatlantic cooperation (EUR-Lex 2021). In a first formulation, the ESDI involves a process that should lead over time to an increase in the role and capabilities of the European Community in managing its own security and beyond. The launch and development of the concept has led to the strengthening of relations between NATO and the EU, which have gradually developed into a partnership with a strong global impact in security and defence matters. The affirmation of the Union in security and defence matters is also seen as a pillar of integrity and effectiveness within NATO. The EU's growing role will not only serve the interests of the Community states, but will strengthen and reinforce transatlantic security and interests over time.

The formation of the transatlantic partnership was a milestone in the evolution of the two entities, but it must be highlighted that despite the efforts of European leaders, the EU's role in crisis management from military perspective remains a minor one. This is due to EU's limited capabilities in terms of armed intervention. Being more dependent on the military capabilities of NATO, the EU should focus more on the soft security component of crisis management, thus becoming a complementary voice for the partnership. Complementarity should not be understood in terms of interoperability, but in terms of complementing the military dimension with what can be post-conflict reconstruction or even conflict prevention through civilian measures. At the same time, the different tools and means they possess can be complementary as long as the two partners aim to ensure collective security by eliminating divergence and duplication of military capabilities. Cooperation is a necessity in these critical times, but especially in the unpredictable future of the international environment: closer cooperation, concerted and joint use and an efficient and transparent European defence sector also strengthen the capabilities available to NATO (European Parliament 2021).

Faced with the same security challenges and threats, NATO and the EU will always look to develop their partnership further with a view to increasing collaboration through continued harmonization of the Euro-Atlantic agenda. Regional instability in the East and South has pushed the EU and NATO to take the initiative to strengthen the partnership, and the 2023 Joint Declaration attests this fact. Only through cooperation and political dialogue can security challenges and threats be limited. Despite this, there are various obstacles of political nature, generated by national interests, public opinion or economic issues concerning defence investment, and the difference in allies' views on global threats and challenges. In addition, these obstacles can also be perceived as elements that may limit the functioning of the partnership as a whole. Perhaps one of the most contentious discussions at the partnership level is around financial issues. The way in which NATO and the EU contribute and allocate their share of GDP to defence and security has been and continues to be a major source of disagreement in the NATO-EU relationship. The United States believes that NATO's functionality also depends on how European states develop their own military capabilities, but especially on their contribution to the Alliance's budget. Continued investment by the Union in particular in strong military capabilities and increased defence funding will not only strengthen the EU, but at the same time the transatlantic alliance, making it a single pole of international power.

The attempt to provide a common response to Russian aggression against Ukraine is in fact a guarantee for strengthening security cooperation between NATO and the EU. The divergences in the partnership's position towards Ukraine, but especially in the economic and military aid offered, can be seen as progress towards a new stage of transatlantic cooperation. It should be noted that the unity of partnership often begins with different visions and contradictions. The best solutions on security and defence issues have been based on contradiction, which is, after all, a form of cooperation. The joint actions and measures taken by both organisations since the beginning of the conflict demonstrate the role that the EU and NATO play in global crisis and conflict management. The sanctions imposed on Russia have emphasised the strength of the partnership, but especially the importance of cooperation in times of maximum intensity. The political dialogue that followed this crisis was focused on restoring balance in Europe, and the assistance offered to Ukraine, both military and civilian, was to discourage escalation of the conflict. Cooperation between NATO and the EU is essential at this critical time for Euro-Atlantic security, and future measures and strategies must be geared towards strengthening the role that the two organisations have developed over time as a stabilising factor in the transatlantic area and beyond.

However, the partners' incapacity to succeed in putting an end to the hostilities between Russia and Ukraine shows that the two organizations need a new approach which includes those aspects that can lead a state to cease hostilities against another

state. As long as there are different positions within NATO and the EU on aid towards Ukraine, on the Russian threat, or even on future actions, or the future of the transatlantic cooperation itself, the actions taken by the two organizations will not stop Russian aggression, but rather it seems more likely that it will intensify it. When all the member states of the partnership, including Hungary – which is taking a stand against the aid actions offered to Ukraine, claiming that military and economic aid is amplifying tensions in the area, and even dragging NATO into a conflict with Russia – will have a unified voice, then there will be better chances for the conflict in Eastern Europe to be stopped. Thus, both NATO and the EU must show more unity on security and defence issues. Only then, will they increase their credibility and become an international force. It is time for the member states of the two organizations to act together and do more than just impose economic or political sanctions.

Comparing all presented aspects, we can strongly affirm that the Transatlantic Partnership is fundamental to stability in the Euro-Atlantic area, and that the strategies and objectives undertaken by both NATO and the EU enhance security at a global level, not just regional. Moreover, the NATO-EU partnership is possible despite political constraints, which means that the two organizations have moved from the discussion phase to working together, focusing on the common goal of security and stability in the transatlantic area. Despite the efforts made over the years to adapt to new security challenges, both NATO and the European Union need to be more assertive when engaging in crisis management.

BIBLIOGRAPHY:

Bogzeanu, Cristina. 2011. "Rolul NATO și al UE în managementul crizelor din Balcanii de Vest." *Centrul de Studii Strategice de Apărare și Securitate.* https://cssas.unap.ro/ro/pdf_studii/rolul_nato_si_al_ue_in_managementul_crizelor_din_balcanii_de_vest.pdf

Chihaia, Mihai. 2024. "Military Mobility: a Stepping Stone for European Defence and Deterrence." *The 7Ds sustainability - Defence Extended, Wilfried Martens Centre for European Studies*, July: 21-27.

Council of the European Union. 2022. "A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international preace and security." *europa.eu.* March 21. https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

Council of the European Union. 2019. "EU Concept for Military Command and Control - Rev 8." *europa.eu, Brussels.* April 23. https://data.consilium.europa.eu/doc/document/ST-8798-2019-INIT/en/pdf#:~:text=The%20EU%20does%20not%20have,missions%20and%20military%20CSDP%20operations

Curtea de Conturi Europeană. 2019. "Document de analiză nr.09 - Apărarea europeană." *europa.eu.* https://www.eca.europa.eu/lists/ecadocuments/rew19_09/rew_eu-defence_ro.pdf

Dungaciu Dan, Cincă Sanda. 2015. *NATO post-Lisabona și provocările regionale.* București: Institutul de Științe Politice și Relații Internaționale.

Duțu, Petre. 2013. *Managementul situațiilor de criză și prevenirea conflictelor armate.* București: Editura Universității Naționale de Apărare "Carol I".

EUR-Lex. 2021. *European security and defence identity.* 06 25. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=LEGISSUM%3Aeuropean_security_defence_identity

EUR-Lex. 2023. *Mutual defence clause.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Amutual_defence.

European Commision. 2023. *European Civil Protection and Humanitarian Aid Operations – 10 years of the Emergency Response Coordination Centre (ERCC).* https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/emergency-response-coordination-centre-ercc/10-years-emergency-response-coordination-centre-ercc_en

European Council. 2024. "EU-NATO cooperation." *europa.eu.* September 2. https://www.consilium.europa.eu/en/policies/defence-security/eu-nato-cooperation/

European Council. 2024. *How the Council coordinates the EU response to crises.* July 3. https://www.consilium.europa.eu/en/policies/ipcr-response-to-crises/

European Council. 2024. *The EU and NATO have further deepened their strategic partnership by jointly responding to common threats and challenges.* 5 June. https://www.consilium.europa.eu/en/press/press-releases/2023/06/16/the-eu-and-nato-have-further-deepened-their-strategic-partnership-by-jointly-responding-to-common-threats-and-challenges/

European Parliament. 2022. "EU strategic autonomy 2013-2023. From concept to capacity." *europa.eu.* July. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733589/EPRS_BRI(2022)733589_EN.pdf

European Parliament. 2021. *Report-A9-0250/2021 on the future of EU-US relations.* 07 26. https://www.europarl.europa.eu/doceo/document/A-9-2021-0250_EN.html

European Union External Action. 2023. *Missions and Operations. working for a stable world and a safer Europe.* 01 23. https://www.eeas.europa.eu/eeas/missions-and-operations_en

Federal Ministry of Defence of the Republic of Austria. 2021. *Handbook on CSDP.* Viena: Armed Forces Printing Center, Volume 1, 4th edition.

Ghiba, Daniel. 2014. *Studiu privind managementul crizelor politico-militare.* București: Editura Universității Naționale de Apărare "Carol I".

Ghiba, Daniela-Mădălina, and Toma Pleșanu. 2018. "Rolul Uniunii Europene în gestionarea crizelor în spațiul european." *Buletinul Universității Naționale de Apărare "Carol I" București*, nr.2: 85-95.

Ghincea, Marius. 2017, actualizat 2022. "Apărarea colectivă și iluzia securității." *Adevărul.ro.* 07 13. https://adevarul.ro/blogurile-adevarul/apararea-colectiva-si-iluzia-securitatii-1797935.html#google_vignette

Groșeanu, Ion-Alexandru. 2013. *Studiu comparativ NATO-UE-OSCE-ONU privind managementul crizelor.* București.

Joja, I. S. 2022. *In the face of Russian aggression, the West needs tu strengthen European security and Black Sea partnerships.* January 11. https://www.mei.edu/publications/face-russian-aggression-west-needs-strengthen-european-security-and-black-sea

Joja, I.S. 2021. *The EU`s East: A way Forward* . March 1. https://www.mei.edu/publications/eus-east-way-forward

Joja, I.S. 2024. *Toward a NATO Black Sea strategy.* July 2. https://www.mei.edu/publications/toward-nato-black-sea-strategy.

NATO. 2022. "NATO 2022 Strategic Concept." *nato.int.* June 29. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO. 2023. "Operations and missions: past and present." *nato.int.* July 10. https://www.nato.int/cps/en/natohq/topics_52060.htm

NATO. 2023. *Operations and missions: past and present.* July 10. https://www.nato.int/cps/en/natohq/topics_52060.htm

Naumescu, Valentin. 2024. *Summit-ul NATO 75 și intrarea Occidentului în Era Războiului Lung.* 07 11. https://www.contributors.ro/summit-ul-nato-75-si-intrarea-occidentului-in-era-razboiului-lung/

Romanyshyn, Iulian. 2021. "Breaking the Law of Opposite Effects: Europe's Strategic Autonomy and the Revived Transatlantic Partnership." *Security Policy Brief, Egmont Institute: Royal Institute for International Relations*, No.140, 1-6. https://www.egmontinstitute.be/app/uploads/2021/03/spb-140-Iulian-Romanyshyn-final.pdf?type=pdf

Sloan, S. R. 2021. "Donald Trump and NATO: Historic Alliance Meet A-historic President." *H-Diplo/ISSF Policy Series, America and the World - The Effects of the Trump Presidency, Middlebury College.* April 8. https://issforum.org/ISSF/PDF/PS2021-20.pdf

DOI: 10.53477/1842-9904-24-9

EU-AFRICA PARTNERSHIP ON PEACE AND SECURITY: A QUEST FOR A STRATEGIC CULTURE?

Andreea DINCĂ*

Amidst the complex, dynamic and highly relevant landscape of the European Union (EU) - Africa relations, the partnership on peace and security constitutes a pivotal aspect, with the EU being an active supporter and substantial funder of national, regional and continental initiatives within this domain.

While the vast majority of current research and debates frame the EU-Africa partnership on peace and security within the context of global power competition, this article explores the potential explanatory role of the strategic culture approach on this topic. Therefore, it looks at the main events and trends influencing the partnership after 2022, assessing whether the EU's security actions in Africa reflect a coherent strategic culture.

The article concludes that the strategic culture framework helps understand European preferences, constraints and effectiveness regarding its security behaviour in Africa.

Keywords: *security; CSDP; EU-Africa relations; strategic culture; strategic compass; APSA.*

Introduction

Although the EU and the African continent have been historically connected since the establishment of the European Economic Community (EEC), the EU-Africa partnership on peace and security was formalised in 2002 with the establishment of the African Peace and Security Architecture (APSA). Moreover, since 2003, when the first Common Security and Defence Policy (CSDP) mission was launched, a vast number of such missions and operations have been deployed in Africa. These work

**** Andreea DINCĂ is a Doctoral Fellow within the European Security and Defence College, and a PhD Candidate at the West University of Timisoara, Romania.***
E-mail: andreea11@gmail.com

in close cooperation and coordination with a multitude of tools and instruments from the EU toolbox aimed at tackling conflicts and crises on the continent.

Given Africa's proximity, historical ties and particular significance for Europe, but also due to the fact that Africa persists as the continent most afflicted by conflicts, with approximately 30% of its population residing in areas affected by conflict, the EU has placed a strong emphasis on the peace and security dimension of its partnership with the continent (4 Sub-Saharan Africa: Regional Analysis, 2023).

In recent years, the global security architecture has encountered critical changes, being affected by a series of events and trends, impacting the security dynamics within the African continent and the overall EU-Africa partnership on peace and security. Globally, following the COVID-19 pandemic, with the war in Ukraine, and more recently, the war between Israel and Hamas, we have witnessed an intensification of global power competition. These events have had a global impact, explicitly affecting the security dynamics across various dimensions within the African continent.

Against this backdrop, characterised by a multiplication of international crises, another trend can be acknowledged when it comes to the African security landscape: the proliferation of international actors whose strategic interests converge towards a more pronounced involvement in managing the security dynamics within the African continent: China, Turkey, India or the Gulf countries (Ekman, 2023; Mishra, 2023; Yaşar, 2022). Moreover, from a regional perspective, the EU-Africa partnership on peace and security has been influenced during recent years by the broader dynamics of EU-Africa relations. These include how the COVID-19 pandemic was managed and the extended post-Cotonou negotiations. Furthermore, the EU-Africa partnership on peace and security has been influenced by internal dynamics. From a European perspective, adopting the Strategic Compass and establishing an innovative financial instrument, the European Peace Facility (EPF), has signalled a shift in the EU's overall approach to international security, influencing its security actions in Africa (Dincă 2023). From an African perspective, the series of coups that the continent has experienced during recent years have severely affected regional and continental dynamics, with Burkina Faso, Mali and Niger leaving the ECOWAS bloc (Obasi 2023).

In light of these multifaceted developments and their crucial implications on the EU-Africa partnership on peace and security, it becomes signally essential to delve more profoundly into these dynamics and assess them from various angles. While current research and debates acknowledge the significance of the topic of the EU-Africa partnership on peace and security, the vast majority of studies assess it from a global power competition perspective (Lanfranchi, 2023; Matisek, 2020; Tadesse Shiferaw & Di Ciommo, 2023). Moreover, a plethora of studies and policy briefs assess the topic while drawing attention to the internal security dimensions within the African continent and their impact on the EU-Africa partnership on peace

and security and the future of CSDP in Africa, pointing towards a crisis of EU's security actions in Africa (Wilén 2023). Therefore, the strategic culture approach is an innovative and comprehensive framework used to explain current and future dynamics beyond historical contingency.

The importance of the strategic culture framework becomes even more significant with the adoption of the Strategic Compass in 2022, whose aim was not only to operationalise the concepts and proposals from the previous EU strategic documents but also to foster the development of a European strategic culture (A Strategic Compass for Security and Defence 2022). Consequently, this paper aims at assessing the EU-Africa relations on peace and security from the perspective of the strategic culture approach. Thus, the article focuses on examining EU security initiatives in Africa from 2022 until the present to evidence whether EU security behaviour in Africa during this timeframe reveals the notion of strategic culture.

By deploying a qualitative design and using primary and secondary data, this study aims to answer the following questions: to what extent do external global events shape the strategic culture underpinning the EU-Africa partnership on peace and security; how do internal dynamics within the African continent affect the EU's strategic culture and security behaviour in Africa; how does the EU's adoption of the Strategic Compass in 2022 influence and foster its strategic culture in Africa; to what extent does the EU security behaviour towards the African continent reflect the emergence of a strategic culture; to what extent do CSDP missions and operations in Africa reveal a thematic consistency and behavioural patterns that are aligned with the EU strategic compass desideratum? Furthermore, this article is grounded in two primary arguments. Firstly, we acknowledge the emergence of a strategic culture guiding the EU-Africa partnership on peace and security. This emergence was catalysed by the adoption and implementation of the Strategic Compass. Secondly, the EU-Africa partnership on peace and security and the overall EU-Africa relations will benefit from an articulated EU strategic culture that arises from colonial approaches and fosters a renewed partnership.

Subsequently, this article comprises four main sections. The first one briefly sets the research context, highlighting the main aspects related to the EU-Africa partnership on peace and security, further highlighting the debate concerning the strategic culture approach and its interpretation in a European context after the adoption of the Strategic Compass. The second section delves into the empirical data, focusing on the EU security behaviour in Africa from 2022 until the present time. The third section discusses the findings, highlighting the main opportunities and challenges for the EU's security actions in Africa. Lastly, the article concludes by stressing the significance of the strategic culture framework in understanding the EU's security behaviour in Africa while suggesting areas for future research to enhance the EU-Africa partnership on peace and security.

1. EU-Africa Partnership on Peace and Security: Strategic Level

1.1. EU-Africa partnership on peace and security: context

When assessing the relationship between the EU and the African continent in terms of peace and security, it is imperative to adopt a comprehensive approach that encompasses multiple dimensions, thereby capturing the intricate nature of this interaction.

From an institutionalist perspective, the partnership reflects the institutional developments that the EU and the African Union (AU) have undergone. These became particularly pronounced starting in the early 2000s when APSA was established. However, the EU-Africa partnership on peace and security is connected to the overall EU-Africa relations framework. This framework has had an evolutionary character, being shaped not only by the EU-Africa agreements but also by the EU's and AU's internal institutional evolution.

The EU-Africa partnership was formally institutionalised in 2000 during the first Africa-EU Summit in Cairo, and it was guided by the Joint Africa-EU Strategy (JAES) signed in 2007 during the Lisbon Summit (Haastrup and Mah 2020). In 2022, during the EU-AU Summit in Brussels, the document A Joint Vision for 2030 is being adopted, a document in which "a renewed and enhanced cooperation on peace and security" is highly emphasised (6th European Union - African Union Summit: A Joint Vision for 2030. 2022).

By this partnership, the EU is mobilising a wide array of tools and instruments to manage the African continent's security dynamics. Acknowledging the security-development nexus, the climate-security nexus, and the challenges posed by illegal migration or disinformation campaigns, the EU employs an integrated approach to security issues in Africa, guided by the principles of human security (Staeger and Gwatiwa 2021). However, the EU's most notable contribution to managing the security dynamics and challenges in Africa is represented by the CSDP missions and operations. Currently, out of 24 CSDP missions and operations, 12 are being deployed in Africa. These will be further explored in the second section of the paper.

Having briefly introduced the context of the EU-Africa partnership on peace and security, the next subsection of the article introduces the overarching framework of the paper, namely the strategic culture one.

1.2. EU and Strategic Culture

Strategic culture is a framework that has been the topic of various debates, with a shared understanding of this approach highlighting its conceptual and theoretical elasticity (Schmidt and Zyla 2013, 2). Moreover, the same authors emphasise that because strategic culture is not strictly defined within any particular international relations theory, it has the potential to yield novel and interdisciplinary insights and results (Schmidt and Zyla 2013, 2).

Strategic culture first appeared as a concept within the context of the Cold War in the 70s, being used in order to explain states' behaviour and decision-making through the lens of culture (Biava, Drent and Herd 2011). In time, the concept evolved, being the subject of debates and even dichotomies about the relation between culture and political action. While recognising that some authors classify the development of this concept into three primary debates or "generations", this paper examines the concept of strategic culture within a European context, particularly concerning the evolution of the EU's security and defence policies, with a focus on the period following 2000 (Schmidt and Zyla 2013, 2). Furthermore, theoretical debates about the nature of the interplay between culture and political action were popular in the early 1990s, thus influencing the evolution of the concept within European milieu (Gray, 1999; Johnston, 1995). However, strategic culture as a framework transcends a mere causal relationship between culture and state decisions, offering the potential to explain state relationships more comprehensively.

Strategic culture can be defined in multiple ways. However, the common denominator of these definitions is that "traditions, values, attitudes, patterns of behaviour, habits, symbols, achievements and historical experiences shape strategic behaviour and actual policy-making" (Toje 2005). With a broad understanding of the concept, it becomes thus evident that the concept lacks certain analytical rigour, as noted by some authors (Biava, Drent and Herd 2011). However, with the appropriate delimitations, the strategic culture approach can offer essential insights, even more so in a European context.

In order to explore and understand the concept of strategic culture in a European context, we need to assess the evolution of this concept within EU milieu. Moreover, since the concept of strategic culture is explicitly mentioned in the Strategic Compass, it is necessary to assess the evolution of the EU's external identity before 2022.

Especially after the establishment of the CSDP and then after the entry into force of the Lisbon Treaty, the European Union entered a new stage in which it became an essential player within the global security architecture by deploying a significant number of CSDP missions and operations. A vast majority of the authors who have approached this topic argue that the power that the European Union projects outside its borders has a soft character (Duchenne, 1972; Manners, 2002; Manners, 2015; Meyer, 2006). Ian Manners (2002; 2006; 2015) starts from the argumentation of Duchene (1972; 1973) and introduces the concept of "normative power Europe" in order to promote the idea of Europe as a normative power and not as a civilising one in world politics.

Monteleone (2016) discusses the emergence of a European strategic culture oriented towards realpolitik and able to define the Union's status as a global actor on the international stage. In his argument, the author uses the opinion of Rogers (2009), who posits the idea that the European Union has had a grand strategy since its

inception, first being oriented towards a civilian power of a soft type, later focusing on aspirations related to the hard power zone. Meyer (2006), in his turn, explores how the strategic cultures of four European countries at that time members of the EU - the United Kingdom, France, Germany, Poland - evolved in the period after the end of the Cold War. Although Member States have to harmonise their various strategic cultures, the conclusion reached is that there is a normative convergence regarding the European strategic culture, consequently witnessing the emergence of what Meyer (2006) calls "Humanitarian Power Europe", in contradiction with the neutrality promoted by a possible "Helvetian Europe", or the pursuit of a global agenda of "Global Power Europe". The traits of the security culture of "Humanitarian Power Europe" are given by the convergence in terms of risk tolerance, resort to force, or support the adoption of missions/operations whose mandate does not go beyond the scope of humanitarian interventions (Meyer, 2006).

In a more recent article, Manners (2006) reconsidered the idea of "normative power Europe" in order to respond to new challenges and to mark a change in the security culture of the Union. Thus, starting from the idea of peace met in Duchene's (1972) works, Manners (2006) advances the idea of "sustainable peace" that emphasises addressing the cause at the expense of symptoms. The author uses the definition given by Peck (1998, 15-16) for sustainable peace, which implies using both short-term problem-solving and long-term structural solutions to conflict prevention through integrating human security concerns and promoting good governance. Referring to the security culture of the EU, Manners (2006) concludes that it took a distinct turn with the adoption of the European Security Strategy (EES) in 2003, focusing now not only on the normative power but on an entire set of tools designed to provide the Union with the ability to act more robustly.

Although the European Union tended to be conceptualised by a vast majority of authors as a "normative power", "quiet superpower", "civilising power", "humanitarian power", or "civil power", in the context of advancing the CSDP, more specifically after the adoption of the Strategic Compass and with the ongoing war in Ukraine, the EU's level of ambition gains new momentum. Therefore, as mentioned explicitly within the text of the Strategic Compass, the concept of strategic culture has become increasingly significant.

Against this backdrop, some authors have explored the framework of strategic culture in relation to CSDP. The vast majority of research conducted before 2022 on the topic is mainly reserved when it comes to developing a military doctrine for the CSDP (Freedman, 2004; Rynning, 2003). Biava et al. (2011) explored the concept in relation to the EU and concluded that the EU's strategic culture has a broad vision of security at its core, referring to the integrated approach to external conflicts and crises.

1.3. Strategic Compass and strategic culture

With the evolution of the global security environment, the European Union has focused on responding to new challenges in this field. Following the launch of the ESS in 2003, the European Union Global Strategy (EUGS) in 2016, in 2020, during the German presidency of the European Council, the *Strategic Compass* was launched.

Preceded by a threat analysis, the document was formally adopted one month after Russia's war against Ukraine started. This event catalysed the adoption of the strategic compass, significantly shaping its content (EEAS Press Team 2023). Essentially, its text focuses on four main pillars (act, secure, invest and partner) and advances over 80 concrete actions in these domains. Moreover, the overall goal of the Strategic Compass was that of fostering a European strategic culture. The path to achieving this objective was facilitated by the development of a comprehensive threat analysis and extensive debates among EU Member States. These discussions aimed at reaching a common understanding of threats and challenges and the strategies to address them (EEAS Press Team 2023).

While acknowledging the return of power politics and the danger that multilateralism might face in such a context, the Strategic Compass provides a common understanding of the strategic environment that the EU is facing. Furthermore, it assesses the current security environment as being "more volatile, complex and fragmented than ever, due to multi-layered threats", identifying the following threats: "hybrid tactics, cyberattacks and foreign information manipulation and interference, economic and energy coercion, an aggressive nuclear rhetoric" as well as "terrorism, violent extremism, organised crime, instrumentalisation of irregular migration, arms proliferation and the progressive weakening of the arms control architecture" (A Strategic Compass for Security and Defence 2022). Thus, one can observe that the definition of security has significantly broadened, with an accent made on hybrid tactics.

The Strategic Compass highlights the players, interests and threats within the EU strategic environment. Concerning Africa, the Strategic Compass identifies ongoing conflicts, poor governance and terrorism as major threats to European security. At the same time, the document points explicitly to regions dealing with challenging security dynamics that need close attention: the Sahel, Central Africa, the Gulf of Guinea, the Horn of Africa and the Mozambique Channel (A Strategic Compass for Security and Defence 2022). A distinguished feature of the Strategic Compass concerning Africa is the emphasis on hybrid threats, namely the instrumentalisation of migrants, disinformation campaigns and the presence of mercenaries groups such as Wagner. Within all these areas, CSDP missions or operations are being deployed, and the Strategic Compass provides concrete measures and actions concerning crisis management.

The "act pillar" from the Strategic Compass focuses on crisis management missions and operations. Its main aim is reinforcing existing CSDP missions and operations by providing them with more robust and flexible mandates backed by a more rapid decision-making process and financial means. The emphasis is being placed on the effectiveness of CSDP missions and operations, and further cooperation with European-led ad hoc missions and operations serving the EU interests being advanced as a possibility. Furthermore, establishing the EPF is presented as an innovative financial framework aiming to bolster CSDP's effectiveness.

Another distinctive feature of the EU security identity is its commitment to multilateralism. This feature is reinforced throughout the text of the Strategic Compass. However, the document places a strong emphasis on partnerships with like-minded actors. Besides reinforcing the already existing strategic partnerships with NATO or the partnerships with the UN, the OSCE, the AU, ASEAN, LAS or GCC, the EU seeks to engage in more robust security partnerships with African partners such as the Regional Economic Communities (RECs) (ECOWAS, SADC, and IGAD) (A Strategic Compass for Security and Defence 2022). Furthermore, tailored bilateral partnerships with some countries are prioritised based on shared values and common interests.

In order to assess the development of the EU strategic culture concerning the EU-Africa partnership on peace and security within the Strategic Compass, we can summarise its strategic goals and aims for the region in five significant dimensions. Firstly, hybrid threats are highlighted. Secondly, existing CSDP missions and operations mandates are subject to revision. Thirdly, the new financial instrument, the EPF, allows for more predictable and flexible financing, thus enhancing capacity building and effectiveness. Fourthly, closer operational ties with RECs are being developed, and security initiatives led by third countries are being financed. Lastly, the commitment to multilateralism in tackling security crises in complex operational environments is being reinforced.

After briefly introducing the context of the EU-Africa partnership on peace and security, conceptualising the strategic culture framework within the EU context and its operationalisation within the Strategic Compass, we will explore the EU-Africa security landscape after 2022 and until the present.

2. EU-Africa Partnership on Peace and Security 2022 - Present

The EU's engagement in Africa within the security domain comprises several lines of action. CSDP missions and operations are the most notable ones. AU-led Peace Support Operations, including RECs peace operations represent the second line of action. The third line of action is represented by EPF assistance measures providing bilateral support to African partner countries. These three lines of action will be further explored in the current section of the article.

2.1. CSDP missions and operations in Africa 2022-present

Currently, out of 24 CSDP missions and operations, 12 are being deployed in Africa: five civilian missions, four military missions, two naval operations and one modular initiative under the CSDP framework that combines military and civilian components.

In order to strengthen the CSDP civilian missions, the EU has adopted in 2023 a new CSDP Compact, consisting of specific guidelines, commitments and lines of action grouped around four pillars, similar to the Strategic Compass ones (act, secure, invest, partner) (EUROPEAN UNION COMMON SECURITY AND DEFENCE POLICY CIVILIAN CSDP COMPACT. Towards more effective civilian missions 2023).

EUBAM Libya has undergone a two-year mandate extension in June 2023. At the same time, the mission's objective was amended from "supporting the Libyan authorities to develop capacity for enhancing the security of Libya's land, sea and air borders in the short term and to develop a broader IBM strategy in the long term" to "enhancing the capacity of the relevant Libyan authorities and agencies to manage Libya's borders, to fight cross-border crime, including human trafficking and migrant smuggling, and to counter terrorism" (Council of the European Union, 2013; Council of the European Union, 2023).

EUAM RCA has also undergone a two-year mandate extension in July 2022. The adopted Council decision introduces a new strategic objective of the mission, namely the support of the strategic communication aimed at promoting European values and exposing human rights violations by foreign forces (Council of the European Union 2022).

EUCAP Mali's mandate was extended for two years on January 10th, 2023, with an additional objective similar to that of EUAM RCA: the support of the strategic communication aimed at promoting European values and exposing human rights violations by foreign forces (Council of the European Union 2023).

EUCAP Niger has undergone a two-year mandate extension on September 9th 2022. While the budget allocated for this period was set to 72 million euros, an additional mission objective was added, namely the development and implementation of a communication strategy aimed at promoting European values in Niger (Council of the European Union 2022).

EUCAP Somalia's mandate was extended for two years on December 13, 2022, while the mission's objectives remained the same (Council of the European Union 2022).

Moving on to the other spectrum of CSDP action in Africa, military missions, three such missions are currently being deployed on the African continent.

EUTM Somalia's mandate has been extended in December 2022 for another two years. The added objective for the new mandate consists of "supporting the development of a Somali-owned Training System" with the final aim of handing over

the training activity to Somali National Army (SNA) by the end of 2024 (Council of the European Union 2022). However, in 2023, through the EPF, the SNA received non-lethal and lethal military equipment, a measure that further operationalises EUTM Somalia's mandate (European Commission 2023).

EUTM RCA was established in 2016 to address the security situation in the Central African Republic (CAR) (Council of the European Union 2020). In 2021, the mission suspended its training activities due to suspicions of trained Central African Armed Forces (FACA) members fighting alongside the Wagner group (Reuters 2021). The Council extended the mandate of EUTM RCA for two consecutive years in July 2022 and in 2023, adding an article according to which the mission will be terminated on September 19th, 2024, subject to a strategic assessment led by the Political Security Committee (Council of the European Union 2023). During this time, the mission has kept its strategic advice pillar to the Ministry of Defence of the CAR and to the FACA General Staff. It has restrained the training one to non-operational domains (European Union Training Mission in Central African Republic 2021).

EUTM Mozambique was established in 2021 with the aim of training and supporting the FADM (Mozambique Defence Armed Forces) in "protecting the civilian population and restoring safety and security in the Cabo Delgado province" (European Union Training Mission in Mozambique 2022). Its mandate was extended until 2026, and at the same time, it is pivoted towards an assistance and advisory mission, transforming itself into EU Military Assistance Mission Mozambique **(**EUMAM Mozambique) as of September 1st, 2024 (Council of the European Union 2024).

Furthermore, there are currently two ongoing naval operations, EUNAVFOR ATALANTA and EUNAVFOR MED IRINI.

In December 2008, the first, the EUNAVFOR Atlanta, was launched as part of a then comprehensive approach of the European Union to the Somali crisis in which piracy was also included. This operation was the Union's short-term response to the Somali crisis. At the same time, in addition to deterring, preventing and repressing acts of piracy, the operation aims to protect UN World Food Programme (WFP) ships delivering humanitarian aid to Somalia and ships transiting Somali territorial waters. At the end of 2022, the operation's mandate has been extended for a two-year time while keeping its central executive and non-executive tasks, and the area of operation has been changed from the "Somali coast" to the West Indian Ocean and the Red Sea (Council of the European Union 2022).

EUNAVFOR Med Irini was launched in March 2020, having as a primary task enforcing the UN arms embargo on Libya. The operation's mandate has been extended twice, the latest extension ending in 2025 (Council of the European Union, 2023).

The latest mission to be deployed within the African continent, EU SDI Gulf of Guinea, has a regional scope of improving stability and resilience of the northern borders of four countries: Cote d'Ivoire, Ghana, Togo and Benin. The

mission's mandate combines capacity building of security and defence forces tasks with operational training for the same forces and "support trust-building between civil society and defence forces" while having a modular and flexible approach in implementing these tasks (Council of the European Union 2023).

Although still ongoing at the time this article was written, the European Union Military Partnership Mission in Niger (EUMPM) Niger will end on June 30 2024. This decision was made by the Political and Security Committee due to the challenging political situation in the country (Council of the EU 2024).

2.2. AU-led Peace Support Operations

Currently, there are ten ongoing AU-led peace operations (PSOs), three of which are AU-mandated, while seven are led by RECs or other regional organisations (G5 Sahel, Lake Chad Basin Commission) and supported by the AU (Allen 2023). With the establishment of the EPF, the PSOs with a military component were financed through this new financial instrument.

During its first two years of implementation, there have been various assistance measures supporting the military components of four AU-led PSOs: 275 million euros for the African Union Transition Mission in Somalia (ATMIS), 20 million euros for the Multi-National Joint Task Force against Boko Haram, 35 million euros for the G5 Sahel Joint Force and 15 million euros for the Southern African Development Community Mission in Mozambique (SAMIM). Additionally, two assistance measures totalling 730 million euros as a general programme to support peace and defence initiatives led by the AU until 2024 (Timeline - European Peace Facility 2024).

Although in June 2023, the Council adopted the decision to extend with 3,5 billion euros the budget of the EPF, the vast majority of the funds (83%) went to supporting Ukraine, while both regional and national measures in Africa counted for 14% of the total budget (Council of the EU 2023) (Bergmann 2023).

Against this backdrop, the United Nations Security Council adopted in December 2023 the resolution 2719, through which it agreed to finance AU-led PSOs (United Nations Security Council 2023).

2.3. Bilateral support to African partner countries

One of the key innovations introduced by the establishment of the EPF is its second pillar, which offers flexibility in bilaterally funding national initiatives in the peace and security domain. Initially, the measure was implemented in Mozambique, the beneficiaries being the units trained by EUTM Mozambique. However, in July 2022, the Council approved an assistance measure worth 25 million euros to support the Nigerien Armed Forces in building a training centre and an operating base (Council of the EU 2022). Still in 2022, the Council has adopted a new decision to

grant assistance measures to the armed forces of the Islamic Republic of Mauritania and to Rwanda Defence Force in Mozambique (Council of the EU 2022).

In 2023, an assistance measure was granted to the 31st Rapid Reaction Brigade of the Armed Forces of the Democratic Republic of the Congo, implemented through the Belgian Ministry of Defence (Council of the EU 2023). From September 2023 – to April 2024, the vast majority of EPF bilateral assistance measures have been granted to countries in West Africa in support of the Beninese Armed Forces, **n**avies of Ghana and Cameroon, Ghana Armed Forces and Armed Forces of Côte d'Ivoire (Timeline - European Peace Facility 2024).

This section of the article provided empirical data for the EU's actions in Africa within the peace and security domain after the Strategic Compass was adopted. The following section will discuss the findings against the strategic culture conceptualisation established in the first section of the article, backgrounded on the empirical data focused on the EU lines of action in Africa since 2022.

3. Discussion: EU-Africa Partnership on Peace and Security and EU Strategic Culture

The EU-Africa partnership on peace and security represents an issue of critical importance, especially in the context of global power competition, the rapidly changing international landscape, and the challenging dynamics of African security.

The Strategic Compass is a relevant strategic document whose aim is, among others, to foster a European strategic culture. Therefore, this article aimed to assess the EU's involvement in Africa within the peace and security domain after the adoption of the Strategic Compass. Moreover, this paper's hypothesis was that the EU security behaviour in Africa during this timeframe reflected common patterns, shared beliefs and strategic preferences that represent the features of a strategic culture. The findings of this article partially validate the hypothesis. Therefore, even if the strategic culture framework represents an analytical lens capable of producing innovative insights, some nuances and limitations have to be addressed concerning this approach. This will be further demonstrated.

Operationalising the main features of the EU security behaviour and aims within this domain as stated in the strategic compass text, we concluded that these could be categorised into five main sections.

The first feature, namely the critical importance of countering hybrid threats, has been addressed directly by the three civilian missions in the Sahel and Central Africa. Thus, these missions' mandates were added a new strategic objective of the mission, namely the support of the strategic communication aimed at promoting European values and exposing human rights violations by foreign forces. This

was the first step in counteracting disinformation campaigns in those operational environments. Moreover, on the websites of all CSDP missions and operations, an information factsheet about the EU Hybrid Toolbox is posted, thus mainstreaming the importance of countering hybrid threats.

During the analysed timeframe, all CSDP missions and operations have undergone mandate extensions. Analysing and comparing the previous mandates against the new ones, we can conclude that with a few exceptions, their revision does not reflect significant changes but mere duration extensions. However, one should stress that the operational environment's security and political contexts influence the mandate revisions, these being established on a case-by-case scenario. Therefore, EUBAM Libya's mandate has been more focused towards tackling security threats that affect the EU's interests, while the civilian missions' mandates from the Sahel and Central Africa have been adjusted so they can better answer to urgent threats in the form of disinformation campaigns against the EU's values and interests.

Another feature of the EU security behaviour is predictable and flexible financing that can enhance CSDP activities' effectiveness and capacity building. This is reflected by the establishment of the EPF, and the assistance measures channelled through it in support of troops trained by EUTM Mozambique and EUTM Somalia. Although through these assistance measures, some capabilities shortfalls of the EUTM missions have been mitigated, and the missions' mandates were operationalised, there is a question mark regarding the future of these missions on the African continent. While EUTM RCA has restrained the training to non-operational domains and the mission will end in 2024, EUTM Somalia envisages the handing over of the training activity to SNA by the end of 2024, and EUTM Mozambique will pivot towards an assistance mission in September 2024. These findings indicate that EUTM missions, once the flagship of CSDP, need a reassessment.

Fourthly, the Strategic Compass advances closer operational ties with RECs and the possibility of bilaterally financing security initiatives led by third countries. As the findings showed, this measure was implemented within the African continent in various contexts. Usually, the assistance measures follow the "train and equip" principle and are intended to enable these partners to autonomously manage their security challenges, thereby contributing to regional stability and reducing the necessity for direct EU intervention. Additionally, these initiatives are complemented by political, diplomatic, and development support and other instruments from the EU foreign policy toolbox. The EU has a broad understanding of security and thus ensures that security assistance is aligned with broader political and economic development strategies.

Lastly, the commitment to multilateralism in tackling security crises in complex operational environments is reinforced throughout the text of the Strategic Compass. In practice, all CSDP missions and operations deployed in Africa closely cooperate

with international partners, while a significant number of mission personnel come from third countries.

The findings further point to the fact that the EU has a distinct feature: a broad understanding of security, just as Biava (2011) rightly pointed out. Moreover, by breaking the barrier of providing assistance measures consisting of lethal equipment to African partner countries – Niger – followed by Somalia, the EU is gradually focusing its engagement within the security domain towards Africa on military capacity-building (Council of the EU 2023). This gradual securitisation of the EU action in Africa marks a shift from the EU's projected image as a signally soft power (Duchenne, 1972; Manners, 2002; Manners, 2015; Meyer, 2006). However, this clear orientation towards securitisation and hard power in Africa does not contradict the normative character of the EU's identity, as these measures are integrated into a broader framework that prioritises human rights, democratic governance, and sustainable development. By balancing hard power with normative principles, the EU continues to promote an integrated approach to peace and security that addresses both immediate and long-term challenges.

The Strategic Compass marks a shift in the development of an EU strategic culture; however, assessing its implementation in a complex environment like the African one is still premature, as only two years have passed since its adoption. This points to a limitation of the current article. Nevertheless, this framework can be further used for longitudinal studies in order to capture the evolution of the EU strategic culture in relation to the EU-Africa peace and security partnership over an extended time. Another direction worth exploring for future studies is a comparative analysis with other regions where the EU is engaged in similar activities.

Conclusion

This article has examined the EU-Africa partnership on peace and security through the lens of the strategic culture approach, assessing the evolution of EU security actions in Africa following the adoption of the Strategic Compass in 2022. The strategic culture framework represents an alternative lens that enables a deep understanding of the EU's security behaviour in Africa while pointing to the preferences, constraints and degree of effectiveness of its actions in the security domain in Africa.

The findings point out the fact that even if, with the adoption of the Strategic Compass, the EU has made a significant step towards aligning its security actions with a strategic culture, its implementation remains in an incipient stage. This is partially due to the short time since the Strategic Compass was adopted and partially due to the evolving yet challenging security dynamics in Africa.

Concerning its CSDP missions and operations in Africa, several conclusions can be drawn. Firstly, especially in the Sahel, civilian missions are mostly kept as "boots on the ground", their main aims are maintaining a presence and a relationship with local authorities. Secondly, the future of EUTM missions in Africa is questionable, pointing to a shift towards an advisory direction or a modular one, as EUTM Mozambique and EU SDI Gulf of Guinea establishment reveal.

Concerning the development of bilateral partnerships in the security domain, funded through assistance measures by the EPF, one can conclude that this constitutes the most profound change in the EU's security behaviour towards Africa. Although after assistance measures are granted to a partner, EEAS carefully monitors that partner's compliance with human rights, international humanitarian and arms export laws, highlighting the measures' normative component, this signals a substantial shift towards a gradual securitisation of the EU action in Africa.

While acknowledging the importance of global security dynamics in shaping the EU-Africa security partnership and the internal security challenges affecting the African continent, the adoption of the Strategic Compass and the establishment of the European Peace Facility mark a shift in the articulation of a European strategic culture, thus shaping the EU's strategic approach to security in Africa.

Despite its limitations concerning this topic, the strategic culture approach offers a promising framework for analysis of the EU-Africa partnership on peace and security, capable of producing innovative insights. While the EU continues to refine and advance its strategic identity, it becomes signally essential to develop a coherent and articulated strategic culture that will contribute to overcoming potential challenges and enhance its partnership with Africa. Moreover, the findings highlight the need for a more nuanced understanding of the EU-Africa partnership. This study underscores the importance of ongoing research and dialogue to strengthen this vital relationship, ultimately contributing to a more secure and stable African continent.

BIBLIOGRAPHY:

—. 2022. "COUNCIL DECISION (CFSP) 2022/1333 of 28 July 2022 amending Decision (CFSP) 2019/2110 on the European Union CSDP Advisory Mission in the Central African Republic (EUAM RCA)." *www.eur-lex.europa.eu.* August 1. Accessed May 20, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022D1333

—. 2022. "COUNCIL DECISION (CFSP) 2022/1505 of 9 September 2022 amending Decision 2012/392/CFSP on the European Union CSDP mission in Niger (EUCAP Sahel Niger)." *www.eur-lex.europa.eu.* September 9. Accessed May 16, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022D1505&qid=1718380556033

—. 2022. "COUNCIL DECISION (CFSP) 2022/2441 of 12 December 2022 amending Joint Action 2008/851/CFSP on a European Union military operation to contribute to the deterrence, prevention and repression of acts of piracy and armed robbery off the Somali coast." *www.eur-lex.europa.eu.* December 12. Accessed May 16, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022D2441

—. 2022. "COUNCIL DECISION (CFSP) 2022/2443 of 12 December 2022 amending Decision 2010/96/CFSP on a European Union military mission to contribute to the training of Somali security forces." *www.eur-lex.europa.eu.* December 12. Accessed May 16, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022D2443#:~:text=(2)%20On%2010%20December%202020,Somalia%20until%2031%20December%202022

—. 2022. "COUNCIL DECISION (CFSP) 2022/2445 of 12 December 2022 amending Decision 2012/389/CFSP on the European Union Capacity Building Mission in Somalia (EUCAP Somalia)." *www.eur-lex.europa.eu.* December 13. Accessed May 16, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022D2445#:~:text=(4)%20In%20the%20context%20of,extended%20until%2031%20December%202024

—. 2022. *European Peace Facility: Council adopts assistance measures in support of the armed forces of five countries.* December 1. Accessed May 20, 2024. https://www.consilium.europa.eu/en/press/press-releases/2022/12/01/european-peace-facility-council-adopts-assistance-measures-in-support-of-the-armed-forces-of-five-countries/

—. 2023. "COUNCIL DECISION (CFSP) 2023/1305 of 26 June 2023 amending Decision 2013/233/CFSP on the European Union Integrated Border Management Assistance Mission in Libya (EUBAM Libya)." *www.eur-lex.europa.eu.* June 23. Accessed May 16, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023D1305

—. 2023. "COUNCIL DECISION (CFSP) 2023/1599 of 3 August 2023 on a European Union Security and Defence Initiative in support of West African countries of the Gulf of Guinea." *www.eur-lex.europa.eu.* August 3. Accessed May 16, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023D1599

—. 2023. "COUNCIL DECISION (CFSP) 2023/653 of 20 March 2023 amending Decision (CFSP) 2020/472 on the European Union military operation in the Mediterranean (EUNAVFOR MED IRINI)." *www.eur-lex.europa.eu.* March 21. Accessed May 16, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023D0653

—. 2023. "COUNCIL DECISION (CFSP) 2023/96 of 10 January 2023 amending Decision 2014/219/CFSP on the European Union CSDP Mission in Mali (EUCAP

Sahel Mali)." *www.eur-lex.europa.eu.* 10 January. Accessed May 16, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023D0096

—. 2023. *European Peace Facility: Council adopts an assistance measure in support of the 31st Rapid Reaction Brigade of the Armed Forces of the Democratic Republic of the Congo.* July 20. Accessed May 20, 2024. https://www.consilium.europa.eu/en/press/press-releases/2023/07/20/european-peace-facility-council-adopts-an-assistance-measure-in-support-of-the-31st-rapid-reaction-brigade-of-the-armed-forces-of-the-democratic-republic-of-the-congo/

—. 2023. *European Peace Facility: Council adopts two assistance measures to support the Nigerien Armed Forces.* June 8. Accessed May 17, 2024. https://www.consilium.europa.eu/en/press/press-releases/2023/06/08/european-peace-facility-council-adopts-two-assistance-measures-to-support-the-nigerien-armed-forces/

2021. "European Union Training Mission in Central African Republic." *www.eeas.europa.eu.* September 15. Accessed May 16, 2024. https://www.eeas.europa.eu/eutm-rca/about-military-training-mission-central-african-republic-eutm-rca_en?s=334

2022. "6th European Union - African Union Summit: A Joint Vision for 2030." *www.consillium.europa.eu.* Accessed May 15, 2024. https://www.consilium.europa.eu/media/54412/final_declaration-en.pdf

2022. "A Strategic Compass for Security and Defence." *satcen.europa.eu.* Accessed May 14, 2024. https://www.satcen.europa.eu/keydocuments/strategic_compass_en3_web6298d4e4601f2a0001c0f871.pdf

2022. *European Union Training Mission in Mozambique.* January 4. Accessed May 16, 2024. https://www.eeas.europa.eu/eutm-mozambique/about-european-union-training-mission-mozambique_en?s=4411

2023. "4 Sub-Saharan Africa: Regional Analysis." *Armed Conflict Survey* 148–253.

2023. "EUROPEAN UNION COMMON SECURITY AND DEFENCE POLICY CIVILIAN CSDP COMPACT. Towards more effective civilian missions." *www.eeas.europa.eu.* May 22. Accessed May 18, 2024. https://www.eeas.europa.eu/sites/default/files/documents/2023/Civilian%20CSDP%20Compact%20Report_22.05.2023.pdf

2024. *Timeline - European Peace Facility.* May 27. Accessed May 27, 2024. https://www.consilium.europa.eu/en/policies/european-peace-facility/timeline-european-peace-facility/

Alcalde, J., D. 2019. "EUTM Somalia: Spain, key factor and commitment." *IEEE Analysis paper* 1-24.

Allen, N., D.,F. 2023. *African-Led Peace Operations: A Crucial Tool for Peace and Security.* August 9. Accessed May 20, 2024. https://africacenter.org/spotlight/african-led-peace-operations-a-crucial-tool-for-peace-and-security/

Bergmann, J. 2023. *Heading in the Wrong Direction? Rethinking the EU's Approach to Peace and Security in Africa.* July 18. Accessed May 20, 2024. https://www.swp-berlin.org/publikation/mta-spotlight-26-the-eu-should-rethink-its-approach-to-african-peace-and-security

Biava, A., M. Drent, and G.,P. Herd. 2011. "Characterizing the European Union's Strategic Culture: an Analytical Framework." *Journal of Common Market Studies* 1-22.

Council of the EU. 2022. *European Peace Facility: Council adopts an assistance measure to support the Nigerien Armed Forces.* July 18. Accessed May 20, 2024. https://www.consilium.europa.eu/en/press/press-releases/2022/07/18/european-peace-facility-council-adopts-an-assistance-measure-to-support-the-nigerien-armed-forces/

Council of the EU. 2023. *European Peace Facility: Council agrees on second top-up of the overall financial ceiling by €3.5 billion.* June 26. Accessed May 20, 2024. https://www.consilium.europa.eu/en/press/press-releases/2023/06/26/european-peace-facility-council-agrees-on-second-top-up-of-the-overall-financial-ceiling-by-35-billion/

Council of the EU. 2024. "EUMPM Niger: Council decides not to extend the mandate of the mission." May 27. Accessed May 27, 2024. https://www.consilium.europa.eu/en/press/press-releases/2024/05/27/eumpm-niger-council-decides-not-to-extend-the-mandate-of-the-mission/

Council of the European Union. 2013. "COUNCIL DECISION 2013/233/CFSP of 22 May 2013 on the European Union Integrated Border Management Assistance Mission in Libya (EUBAM Libya)." *www.eur-lex.europa.eu.* May 24. Accessed May 16, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D0233

Council of the European Union. 2017. "COUNCIL DECISION (CFSP) 2016/610 of 19 April 2016 on a European Union CSDP Military Training Mission in the Central African Republic (EUTM RCA)." *eur-lex.europa.eu.* June 8. Accessed May 16, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016D0610-20170608&from=EN

Council of the European Union. 2020. "COUNCIL DECISION (CFSP) 2020/1133 of 30 July 2020 amending Decision (CFSP) 2016/610 on a European Union CSDP Military Training mission in the Central African Republic (EUTM RCA)." *eur-lex.europa.eu.* 7 31. Accessed May 16, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020D1133&rid=9

Council of the European Union. 2023. "COUNCIL DECISION (CFSP) 2023/1600 of 3 August 2023 amending Decision (CFSP) 2016/610 on a European Union CSDP Military Training Mission in the Central African Republic (EUTM RCA)." *www.eur-lex.europa.eu.* August 3. Accessed May 16, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023D1600

Council of the European Union. 2024. "COUNCIL DECISION (CFSP) 2024/1354 of 14 May 2024 amending Decision (CFSP) 2021/1143 on a European Union Military Training Mission in Mozambique (EUTM Mozambique)." *www.eur-lex.europa.eu.* May 15. Accessed May 16, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401354

Davis Cross, M., K. 2011. "Europe, a smart power?" *International Politics* 691-706.

Dincă, A. 2023. "The European Peace Facility in action: rethinkingEU-Africa partnership on peace and security?" *Political Studies Forum* 123-144.

Duchenne, F. 1972. "Europe's role in world peace." In *Europe tomorrow: sixteen Europeans look ahead*, by R. (ed) Mayne, 32-47. London: Fontana.

Duchenne, F. 1973. "The European Community and the uncertainties of interdependence." In *A nation writ large? Foreign policy problems before the community*, by M. Kohnstamm and W. (eds) Hager, 1-21. London: Macmillan.

EEAS Press Team. 2023. *Questions and answers: a background for the Strategic Compass.* March 20. Accessed May 16, 2024. https://www.eeas.europa.eu/eeas/questions-and-answers-background-strategic-compass-0_en

Ekman, A. 2023. "China's Global Security Initiative. When the process matters more than the content." *European Union Institute for Security Studies.* March. Accessed May 12, 2024. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_5_China%27s%20Global%20Security%20Initiative.pdf

European Commission. 2023. *EU-Somalia: first hand-over of non-lethal military equipment funded by the European Peace Facility takes place in Mogadishu.* July 6. Accessed May 16, 2024. https://fpi.ec.europa.eu/news/eu-somalia-first-hand-over-non-lethal-military-equipment-funded-european-peace-facility-takes-place-2023-07-06_en

Freedman, L. 2004. "Can the EU develop an effective military doctrine?" In *A European Way of War*, by S. Everts, L, Freedman, F. Heisbourg, D. Keohane and M. O'Hanlon. London: Centre for European Reform.

Gray, C.,S. 1999. "Strategic Culture as Context: The First Generation of Theory Strikes Back." *Review of International Studies* 49-69.

Haastrup, T., and L. (eds.), Duggan N. Mah. 2020. *The Routledge Handbook of EU-Africa Relations.* London: Routledge.

Johnston, A.,I. 1995. "Thinking about Strategic Culture." *International Security* 32-64.

Kaunert, C., and K. Zwolski. 2013. *The EU as a global security actor: a comprehensive analysis beyond CFSP and JHA.* Basingstoke: Palgrave Macmillan.

Lanfranchi, G. 2023. *The European Union in a crowded Horn of Africa.* December 19. Accessed May 14, 2024. https://www.clingendael.org/publication/european-union-crowded-horn-africa

Manners, I. 2002. "Normative power Europe: a contradiction in terms?" *Journal of Common Market Studies* 40 (2): 235-258.

Manners, I. 2002. "Normative power Europe: a contradiction in terms?" *Journal of Common Market Studies* 40 (2): 235-258. doi: https://doi.org/10.1111/1468-5965.00353

Manners, I. 2006. "Normative power Europe reconsidered: beyond the crossroads." *Journal of European Public Policy* 13 (2): 182-199. doi: https://doi.org/10.1080/13501760500451600

Manners, I. 2015. "The European Union in global politics: normative power and longitudinal interpretation." In *Research methods in European Union studies*, by K. Lynggaard, I. Manners and K. (eds) Lofgren, 221-236. London: Palgrave Macmillan.

Matisek, J. 2020. "International Competition to Provide Security Force Assistance in Africa: Civil-Military Relations Matter." *Prism* 102-113.

Meyer, C. 2006. *The quest for a European strategic culture: changing norms on security and defence in the European Union.* Basingstoke: Palgrave Macmillan.

Mishra, A. 2023. "Boosting India-Africa defence and security partnership." *Observer Research Foundation.* March 24. Accessed May 12, 2024. https://www.orfonline.org/expert-speak/boosting-india-africa-defence-and-security-partnership

Monteleone, C. 2016. "Beyond material factors? Identity, culture and foreign and security policy of the EU." In *International relations theory and European security*, by C. Cladi and A. (eds) Locatelli, 83-99. London: Routledge.

Moravcsik, A. 2010. "Europe: The Second Superpower." *Current History* 91-98.

Obasi, N. 2023. *ECOWAS, Nigeria and the Niger Coup Sanctions: Time to Recalibrate.* December 5. Accessed May 13, 2024. https://www.crisisgroup.org/africa/sahel/niger/ecowas-nigeria-and-niger-coup-sanctions-time-recalibrate

Peck, C. 1998. *Sustainable peace: the role of the UN and Regional Organizations in preventing conflict.* Lanham,MD: Rowman&Littlefield.

Reuters. 2021. *EU suspends military training in Central Africa over Russian mercenaries.* December 15. Accessed May 16, 2024. https://www.reuters.com/article/eu-centralafrica-security-idAFL8N2T0586/

Rogers, J. 2009. "From "civilian power" to "global power": explicating the European Union's "grand strategy" through the articulation of discourse theory." *Journal of Common Market Studies* 831-862. doi:https://doi.org/10.1111/j.1468-5965.2009.02007.x

Rynning, S. 2003. "The European Union: Towards a Strategic Culture?" *Security Dialogue* 479-496.

Schmidt, P., and B. Zyla. 2013. *European Security Policy and Strategic Culture.* Abingdon: Routledge.

Staeger, U., and T.,T. Gwatiwa. 2021. "Peace and security in the context of EU-Africa relations." In *The Routledge Handbook of EU-Africa Relations.*, by T. Haastrup, L. Mah and N. (eds.) Duggan, 175-187. Abingdon: Routledge.

Tadesse Shiferaw, L., and M. Di Ciommo. 2023. *Trouble in paradise: The EU-Africa partnership in a geopolitical context.* November 13. Accessed May 14, 2024. https://ecdpm.org/work/trouble-paradise-eu-africa-partnership-geopolitical-context

Toje, A. 2005. "Introduction: The EU Strategic Culture." *Oxford Journal on Good Governance* 9-16.

United Nations Security Council. 2023. "Resolution 2719 (2023)." *www.un.org.* December 21. Accessed May 20, 2024. https://documents.un.org/doc/undoc/gen/n23/420/06/pdf/n2342006.pdf?token=ao7OAfBXwF0Jr5qDDt&fe=true

Wilén, N. 2023. *Have African Coups provoked an Identity Crisis for the EU?* December. Accessed May 14, 2024. https://www.egmontinstitute.be/app/uploads/2023/12/Nina-Wilen_Policy_Brief_323_vFinal2.pdf?type=pdf

Williams, P., and H., Y. Ali. 2020. "The European Union Training Mission in Somalia: an assessement." *SIPRI Background Paper* 1-20.

Yaşar, N., T. 2022. "Unpacking Turkey's Security Footprint in Africa Trends and Implications for the EU." *Stiftung Wissenschaft und Politik.* June 30. Accessed May 12, 2024. https://www.swp-berlin.org/10.18449/2022C42/

DOI: 10.53477/1842-9904-24-10

DOCTRINAL APPROACH TO GAIN SEABED CONTROL – THE CASE OF BLACK SEA SECURITY

Lucian Valeriu SCIPANOV*
Marian-Vasile SAVA**

The paperwork examines the complex seabed environment to emphasize the importance of gaining seabed control as part of the broader maritime security. The article demonstrates the importance of researching what the concept of "seabed warfare" means to suggest some directions for the seabed warfare doctrine alone or as part of a naval doctrine. The research aims at identifying the key directions necessary for achieving seabed control and its potential to integrate seabed warfare concepts into the naval doctrine. Therefore, the first part of the article highlights the geophysical, military, and economic characteristics of the seabed environment relevant to seabed warfare. The second part of the paper aims to provide some directions for obtaining seabed control, and a classification system for seabed warfare operations.

The novelty of the article lies in the identification of the seabed control directions and the opportunity to integrate the seabed control concept into the Romanian Naval Forces doctrine.

Keywords: *seabed warfare; naval doctrine; maritime control; seabed surveillance; underwater operations.*

Introduction

Considering the concern of the main Euro-Atlantic and regional actors regarding the security of the maritime borders, there is an inherent need to broaden the contribution of member states to strengthening the protection of the Black Sea. A

**** Captain (N) Lucian Valeriu SCIPANOV, PhD, is a Professor within the Naval Forces Department, Command and Staff Faculty, "Carol I" National Defence University, Bucharest, Romania. E-mail: shcipio@yahoo.com***
***** Marian-Vasile SAVA is a LTJG, Engineer, Romanian Naval Forces. E-mail: vasile.sava@navy.ro***

less addressed component at the community level concerns seabed security. Due to the depreciation of maritime security in the Black Sea region, it is appropriate to pay more attention to this domain. Thus, in this article the research is directed towards the seabed security field. In the authors' opinion, seabed security is a component of maritime security that presupposes a more detailed control of the underwater environment, in terms of the control and safe exploitation of seabed opportunities. From this perspective, it can be considered appropriate to address the issue of seabed security as part of a Black Sea security strategy. Moreover, it is necessary to review the doctrine of the Euro-Atlantic naval forces, including the Romanian Navy doctrine in the seabed warfare approach, considering the new security challenges with effects on actions in the tactical environment.

The study tackles several key objectives, namely to identify the directions necessary to gain effective seabed control and explore the potential to integrate these concepts into Navy doctrine. These objectives are vital for enhancing the capabilities of the Romanian Navy and ensuring that they are prepared to face contemporary and future maritime challenges. The article provides a roadmap for integrating seabed warfare concept into the Romanian Navy doctrine. The insights and recommendations presented in this study can play a pivotal role in modernizing maritime strategy, enhancing operational capabilities, and ensuring the continued security and control of the Romanian Navy in the increasingly contested maritime environment.

A thorough analysis of strategies in the field of seabed security has been carried out, with a focus on the approaches of some EU states, but not only, those with advanced concerns in the field, such as England, France, or Italy, so that these approaches can constitute an inspiration model for a seabed security strategy for Romania. The result of this analysis identifies some conclusions that will emphasize common elements and the differences in the points of view of the schools of thought on seabed security. Moreover, the expectation is to identify, if any, specific characteristics of the concept in order to take over and apply it in the particular case of the seabed security of the Black Sea.

The first part of the article provides a brief analysis of the seabed environment, focusing on the characteristics that are most relevant to seabed warfare. It discusses the unique physical, geological, and ecological aspects of the seabed that impact military operations, including terrain features, resource distribution, and potential hazards. This section lays the groundwork for understanding how the seabed environment can be both a strategic advantage and a challenge in underwater combat scenarios.

In the second part, the paper outlines three strategic directions to follow in order to achieve effective seabed control. These directions encompass technological advancements, tactical approaches, and policy recommendations. Each direction is

explored, offering insights on how modern naval forces can leverage new technologies and methodologies to dominate the seabed and ensure security and superiority in this domain. The discussion includes examples of current technologies and future developments that could play a critical role in seabed control.

The final part of the article presents the inductive definition of seabed security and seabed warfare in terms of maritime environment control. These conceptual definitions will offer an understanding of a context in which the Romanian Navy should plan, execute, and integrate actions into seabed warfare. The goal is to seamlessly incorporate seabed warfare into the existing naval doctrine, ensuring that it becomes a core component of Navy capabilities.

The novelty of this article lies in its innovative approach to identifying the key directions necessary to achieve seabed control and its potential for integrating these concepts into the Romanian Navy doctrine. By providing a clear framework and some actionable recommendations, the article not only advances the theoretical understanding of seabed warfare but also offers practical steps for enhancing the operational capabilities of the Romanian Navy. This integration represents a significant step forward in developing seabed warfare principles, defining a modern maritime strategy and ensuring maritime security in the increasingly contested underwater domain.

1. The Seabed – a Complex Environment

Considering the geographical complexity of the Black Sea in the vicinity of the Romanian coast, concerning the existence of various critical infrastructures such as submarine cables (communication cables), and gas or oil pipelines from maritime drilling platforms, it is necessary to pay more attention to the security of the maritime area, and implicitly on the seabed. Beyond that, if we look to the future and take into account the projects in different stages of development or implementation, such as wind and hydro fields, aquaculture farms, and submersible platforms, the issue of seabed security is topical with projection to the near and distant future alike.

If it is taken into account that from a military point of view, the continental shelf is part of the area of responsibility of the Romanian naval forces, a delegation of competence for a new mission of the naval forces, ensuring seabed security, is foreshadowed.

For the development of the research, geophysical, military and economic descriptors and indicators were used, with the help of which the identification of some particularities of the seabed environment was followed, so that later it could be possible to identify ways to control the security of this environment.

Firstly, in terms of geophysical structure, the seabed encompasses vast areas of different depths. These depths can range from shallow coastal regions to deep

trenches. Depth variations are influenced by factors such as continental shelf width, tectonic activity, and sea currents. Coastal areas tend to have shallower depths, while offshore regions can be significantly deeper. The depth of the seabed has important implications for marine life, water circulation patterns, and human activities such as shipping, fishing, and resource exploration. The composition of the seabed varies widely depending on factors such as location, geological history, and sedimentation processes. In coastal areas, the seabed may consist of sandy beaches, rocky outcrops, or muddy estuaries. Offshore regions often feature sedimentary deposits, including mud, silt, sand, and gravel. These sediments accumulate over time through processes such as erosion, deposition, and biological activity. The composition of the seabed can also be influenced by human activities, such as dredging, mining, and pollution, which can alter sediment dynamics and ecosystem health.

Secondly, analysing from the military point of view, the seabed, due to its inherent characteristics, introduces a new tactical framework associated with a form of ambiguity. This comes from the challenge of operating a vast, obscure, and scarcely accessible domain but also from the dares of monitoring it. These challenges regarding the underwater operations are also detailed by the Instituto Affari Internazionali – a famous Italian think tank (Calcagno Elio 2023). After studying some of the literature on this subject, it can be stated that, being so difficult to operate in this environment due to pressure, visibility, lack of technology, and so on, a precarious exercise of authority arises. The inherent characteristics of this environment, coupled with limited monitoring resources, foster secrecy and render actions challenging to define. The nature of this environment encourages concealment and makes attributing actions difficult. Hybrid strategies may consequently arise, intertwining clandestine commercial, scientific, and military activities that defy easy attribution (Parly 2022). Consequently, the military domain must pay more attention to the seabed security domain and identify the most appropriate measures to control the activities on the seabed. This aspect would include active actions toward the objective but also a doctrinal approach, including the development of combat capabilities in the field (Clark Bryan 2020). Thus, seabed warfare is foreshadowed as an independent domain in the underwater warfare domain.

Finally, economically, the seabed offers countries bordering the seas some unique opportunities for industry and development. The seabed holds valuable resources such as oil, gas, minerals, and even marine life. Extracting these resources requires advanced technology and major investments. In addition, exploiting these resources often involves navigating complex regulatory frameworks and international agreements. Exploitation of seabed resources can have significant environmental consequences. Activities such as deep-sea mining can disrupt fragile ecosystems, damage habitats, and affect marine biodiversity. Balancing economic interests with environmental concerns requires thorough assessments and mitigation strategies,

which can add complexity and cost to seabed operations. Developing and deploying the infrastructure required for seabed operations, such as drilling platforms, oil and gas pipelines, cables, etc., requires sophisticated engineering and logistical expertise. Having these arguments regarding the economic value of the seabed, we can emphasize the importance of managing the control of this environment and maintaining its security.

In summary, after a short description of the geophysical structure, military, and economic point of view, it can be stated that the seabed is a complex environment. Understanding those characteristics is essential for managing seabed control. The challenges of operating underwater were also presented, including limited visibility, extreme environmental conditions and the potential for hybrid events. The economic importance of the seabed cannot be neglected due to development opportunities. This is the starting point from which to affirm the Navy's role and the chance to develop seabed warfare capabilities.

2. Seabed Control as Part of Maritime Security

The previous sections constitute the base for establishing the way in achieving the control of the underwater domain; its complexity dictates the roadmap from planning to conduct naval operations in this unique environment. The seabed control could be defined as the ability to assert influence and sovereignty over the underwater domain which is important for protecting national interests, securing maritime borders, and ensuring access to strategic resources (Carr Christopher J. 2018). Starting from the definition of seabed control, a definition of seabed security can be formulated.

Seabed security definition

It is the authors' opinion that seabed security is a component of maritime security which involves a more detailed control of the underwater environment, in terms of seabed infrastructures control and the safe exploitation of seabed resources.

Next, in order to define the concept of "seabed warfare", an introspection is required on the challenges of the naval forces in this field. The Romanian Navy interest zone includes the underwater domain but is there a well-defined doctrine as to seabed warfare?

Not being a dedicated one, and as a result of studying and analysing specialized works and articles related to this field, three directions have been identified and can be proposed, which certify that the Romanian Navy should consider the following to achieve seabed control:

a) expertise of the seabed through the examination of physical characteristics;

b) surveillance of the seabed and underwater environment;

c) conduct operations on, from, and towards the seabed.

Considering the complex physical attributes of the submarine domain (Sava 2024) - an inherently opaque, challenging to access, expansive, and largely uncharted environment - the resolution to these three operational needs must be formulated within a well-defined spatial framework. This framework should align seamlessly with the perceived threat level and the capabilities and effectiveness of our resources.

In the following section, will be illustrated the significance of each proposed direction in achieving effective seabed control. By delving into the tactical importance and specific advantages of each approach, will be demonstrated how they collectively contribute to the endeavour's overarching goal. Understanding these directions will not only clarify their roles but also highlight their synergistic effect in securing the underwater domain. As they address various aspects, each proposed direction is crucial for this endeavour.

In terms of the expertise of the seabed examination of physical characteristics, acquiring a comprehensive understanding of the seabed and its immediate surroundings is a fundamental prerequisite for ensuring safety, autonomy, and effectiveness in maritime operations. Beyond underpinning our sea control capabilities, this crucial comprehension of the environment is integral to a broader strategy aimed at readiness for threat assessment, establishing response strategies, and enhancing the efficacy of defence. Therefore, advancing our knowledge of the seabed entails honing our capacity to measure, characterize, and analyse the physical parameters of the underwater environment.

Understanding what the seabed is necessitates the capability to keenly identify any magnetic or electromagnetic anomaly within and upon it. Magnetic or electromagnetic detection techniques, relying on contrasts in magnetic and electrical resistivity, show potential and merit development to effectively onboard sensors. Enhancing magnetic mapping and detection methods for man-made objects ought to be a priority for the Maritime Hydrographic Directorate.

In terms of seabed and underwater environment surveillance, to uphold the operational freedom of our forces and protect Romanian national interests, notably including the defence of our vital submarine infrastructures, it is imperative that during peacetime to independently identify and characterize any human underwater activity on the seabed. We consider it self-evident, as it is emphasized in specialized works (Scipanov 2020), the importance of permanent surveillance of the underwater environment in times of peace, crisis, or war.

Consequently, there is a need to enhance our capacity to monitor, detect, and precisely locate potential threats present on the seabed (such as mines, sabotage explosives, fixed or semi-fixed surveillance networks, etc.), which could obstruct the freedom of operation of our armed forces or compromise critical infrastructure

integrity. To ensure effectiveness, credibility, and alignment with our national aspirations, the seabed monitoring capability in question must closely align with our national interests.

Seabed monitor operations will depend on deploying a range of complementary assets, including hull-mounted or towed sonar, unmanned underwater and surface vehicles, as well as sonobuoys. These assets can be launched from specialized naval and air-maritime platforms to cover a vast bathymetric range, spanning from shallow to deep waters. Given the diverse bathymetry of the areas of interest previously mentioned, the capability to operate at depths of up to 2,000 meters aligns with our commitment to maintain the operational freedom of our forces and contribute effectively to the monitoring and protection of submarine critical infrastructure and national interests. Achieving accurate detection and classification of small devices in deep waters, such as attack vehicles, listening devices, or acoustic sensors, necessitates precise measurement capabilities that can only be achieved with underwater vehicles (AUVs, ROVs) operating in close proximity to the seabed and equipped with accurate sensors (Clark 2015).

Analysing the opportunity of establishing an underwater surveillance network positioned on the seabed serves multiple military purposes: safeguarding maritime approaches, bolstering force projection endeavours, and deterring potential enemies (Marcus Solarz Hendriks 2024). This capability can be achieved through a combination of fixed, semi-fixed, or mobile devices – such as seabed antennas, surveillance equipment, AUVs, and gliders – strategically distributed and configured based on operational requirements, environmental factors, and threat assessments (Johannes Peters 2021). Evaluating the feasibility of deploying an underwater surveillance system in our maritime approaches and integrating it with existing anti-submarine warfare assets (such as surface ships, mine countermeasure capabilities, and anti-submarine aircrafts) underscores our commitment to enhancing maritime security. Before committing to such a sophisticated military asset, comprehensive technical and operational studies are essential to master the underlying technologies and evaluate their acoustic detection capabilities. Beyond bolstering anti-submarine defences, this capability can contribute to a broader strategy of safeguarding national interests and enhancing resilience by enabling continuous monitoring and early warning of potential threats to our submarine critical infrastructure.

The primary focus of seabed warfare should be on the following area:

- territorial waters;
- the Romanian EEZ;
- any operational area (important for the freedom of action of Romanian forces and safeguarding our national interests).

If from a military point of view, the continental shelf is part of the area of responsibility of the Romanian naval forces, a delegation of competence for a

new mission of the naval forces, the seabed warfare, ensuring seabed security, is foreshadowed.

In the view of the above, we can further formulate a structured definition of seabed warfare.

Seabed warfare definition

In the authors' opinion, seabed warfare represents the totality of the specialized fleet capabilities' action measures in the maritime environment, developing the ability to operate effectively at the bottom of the sea and deep waters, whether through presence, surveillance, proactive anticipation soft and hard measures, in response to risk and threats, employing a spectrum of actions, passive or active, ranging from discovery, classification, reconnaissance and attack to the infrastructures protection, retrieval and salvage of some objects or submarine vehicles.

Aligned with our national vision for maritime surveillance, the seabed warfare capabilities will enhance the operational capacity in maritime security ensuring the preservation of the Navy's freedom of action and the protection of critical infrastructure, primarily concentrating on the territorial waters zone and the Exclusive Economic Zone (EEZ).

The capability to operate effectively in the deep waters of the Black Sea aligns with the imperative to assert control over maritime domains and aligns with the advancement of underwater surveillance systems. As accessibility to the sea floor expands to include a wider range of actors operating at increasingly greater depths, it becomes imperative for us to explore deeper uses of undersea capabilities. Consequently, our capacity for deep-sea interventions must adapt to this evolving reality, emphasizing the importance of being able to conduct occasional operations directly from the seabed (Stöhs 2021).

It is the authors' belief that the three directions previously presented represent the essence of seabed control as part of the broader maritime security. To follow these directions, the Romanian Navy should consider acquiring the capabilities needed to be able to operate in this complex underwater domain. For this, it is necessary to take into account the doctrinal, knowledge, technological, financial resources, and specialized personnel aspects. Moreover, it is needful to integrate a vision of the necessary, existing, or developing capabilities. Given the actual state of the Romanian Navy, it is necessary to implement a resilience transformation plan.

Conclusions

In conclusion, it has been underlined the complexity and importance of the seabed environment from geophysical, military, and economic perspectives. By examining its intricate geophysical structure, conducting thorough military

assessments, and performing detailed economic analyses, it has been highlighted the multifaceted significance of this critical domain. This approach underscores the necessity of integrated military strategies to effectively manage and utilize seabed resources, ensuring both national security and economic prosperity.

Regarding the approach presented, new concerns arise among the decision-makers in maritime security regarding the development of a new strategic security direction in the field. Starting from this direction, the Romanian Navy will be forced to act on two forecasting levels. A doctrinal one, which will enable dedicating a special chapter for seabed warfare and a chapter for developing capabilities to action in the field. A capability development one, with a careful analysis of the need to develop the future capabilities of the Romanian Navy is suggested, as well as the training of specialized personnel who can operate these capabilities.

Therefore, based on the complexity of the underwater domain, the three proposed directions encapsulate the core elements of seabed control within the context of broader maritime control. Embracing these directions necessitates that the Romanian Navy equip itself with the requisite capabilities to effectively operate within this intricate domain. This entails a holistic approach encompassing technological advancements, robust knowledge acquisition, and investment in skilled human resources. Given the current state of the Romanian Navy, a comprehensive transformation plan must be implemented to address these evolving requirements. Such a plan should prioritize the enhancement of technological infrastructure, the expansion of specialized expertise, and the cultivation of a proficient workforce capable of navigating the complexities of seabed operations. By undertaking this transformative endeavour, the Romanian Navy can position itself as a formidable presence in safeguarding national interests and contributing to regional maritime security.

To achieve the performance to conduct all three functions mentioned in the last part of the paper, the Romanian Navy has to follow a large endowment program. Examples of modern equipment that the Navy should consider acquiring can be hydrographic maritime drones that can carry multiple sensors for underwater research and surveillance, mine warfare systems with the ability to detect, classify, localize, identify, and neutralize drifting mines, midget submarines that can infiltrate into the enemy area of interest and collect data, medium size diesel-electric submarines for intel ops and attack potential enemies and (semi-)fixed seabed surveillance sensors.

As the importance of the seabed continues to increase, questions arise regarding its role within multidomain operations. While the seabed is not a discrete compartment or domain in itself, it represents a new and potentially contentious arena for conflicts, demanding vigilant monitoring and specialized strategic planning.

Integrating the subject of seabed security and seabed warfare into the overarching doctrine of naval forces extends beyond mere recognition and description of operations, as previously outlined. It requires the development of a distinct body

of doctrine that outlines the framework, principles, and tools essential for effective naval operations in this unique environment. This doctrine must remain adaptable to ongoing technological advancements, addressing critical areas such as submarine communications, energy extraction, underwater vehicle utilization, and more. By doing so, the Navy can effectively navigate the complexities of seabed warfare and maintain strategic superiority in this evolving maritime domain.

We believe it is appropriate to affirm that the article achieved its intended objectives. Moreover, it goes beyond by not only advancing the theoretical understanding of seabed warfare but also by providing tangible steps for enhancing the operational and doctrinal framework capabilities of the Romanian Navy. This integration signifies a noteworthy contribution brought forth by this article.

BIBLIOGRAPHY:

Calcagno Elio, Cosentino Michele, Freyrie Michelangelo, Marrone Alessandro, Nones Michele. "The Underwater Environment and Europe's Defence and Security." *Instituto Affari Internazionali, Italy*, 2023: 9-11.

Carr Christopher J., Franco Jahdiel, et al. *Seabed Warfare and the XLUUV.* Systems Engineering Capstone Report, Monterey: Naval Postgraduate School, 2018.

Clark Bryan, Cropsey Seth, Walton Timothy A. *Sustaining the Undersea Advantage: Disrupting Anti-Submarine Warfare Using Autonomous Systems.* Washington: Hudson Institute, 2020.

Clark, Bryan. *The Emerging Era in Undersea Warfare.* Studies, Centre of Strategic and Budgetary Assessments, p.16, 2015, 16.

Johannes Peters, Pawlak Julian. *Below the Surface: Undersea Warfare Challenges in the 21st Century, From the North Atlantic to the South China Sea.* Seapower Series, Baden-Baden: ISPK, Nomos, 2021.

Marcus Solarz Hendriks, Harry Halem. *From space to seabed: Protecting the UK's undersea cables from hostile actors.* 02 19, 2024.

Parly, Florence. *https://www.vie-publique.fr/discours/283847-florence-parly-14022022-maitrise-des-fonds-marins.* 02 14, 2022.

Sava, Marian Vasile. "Analysis of submarine operations in semi-enclosed seas – the Black Sea." *The 20th International Sciencific Conference Strategies XXI.* Bucharest: Carol I National Defence University, 2024. 211.

Scipanov, Lucian Valeriu, Dolceanu Denis. "The oportunity for using remotely operated underwater vehicles in support of naval actions." *Buletin of Carol I National Defence University, NDU "Carol I" Publishing House,* Bucharest 2020, Issue Vol. 9 no. 3, 2020: 62-69.

Stöhs, Jeremy. "How High? The Future of European Naval Power and the High-End Challenge." *Centre for Military Studies,* Denmark, 2021.

DOI: 10.53477/1842-9904-24-11

LEVERAGING EMERGING AND DISRUPTIVE TECHNOLOGIES TO STREAMLINE THE DEPLOYMENT PROCESS AND ENHANCE FORCE PROTECTION IN CURRENT AND FUTURE OPERATING ENVIRONMENT

Ionela Cătălina MANOLACHE*

The current security environment requires precise and adjusted protection measures provided by security-generating organizations. Protecting the transatlantic area is an international priority, and emerging and disruptive technologies are crucial. However, to secure this area, it is essential to adopt effective force protection measures and credible force projection during deployment. Through specific research practices, such as documentary analysis, the paper intends to address how military leaders organize the rapid movement of forces to potential "hotspots" by planning for force protection and leveraging emerging and disruptive technologies.

***Keywords**: deployment; force protection; emerging and disruptive technologies; security; critical infrastructure; movement.*

Introduction

Multiple threats to international security constitute a challenge to national security, and there are several factors, such as political instability, economic inequities, climate changes, cyber security threats, nuclear proliferation, or the outbreak of conflicts, that facilitate the development of an unsafe, unstable, and vulnerable operating environment.

**** Captain Ionela Cătălina MANOLACHE is a PhD Student within the "Carol I" National Defence University, Bucharest, Romania, and Staff Officer within the Headquarters Multinational Division South-East, Bucharest, Romania.***
E-mail: catalinagrigore2694@gmail.com

In 2024, the conflicts in Ukraine and Gaza Strip could significantly alter the global geopolitical landscape, reconfiguring international and regional dynamics and causing worldwide instability and uncertainty. The costs of these conflicts are staggering. Therefore, the primary objective is to prevent their escalation and expedite the return to peace (Zhang, 2024).

At the national level, it is stipulated in the *National Defence Strategy for 2020-2024,* the idea that "*the security environment is characterized by an extensive reconfiguration of relations between actors with global interests, a fact that can influence the stability and predictability of the international system*". Russian Federation's unjustified and violent actions towards Ukraine and its violation of the norms of international law represent an imminent danger to the security of the transatlantic area (Administrația Prezidențială, 2020). For these reasons, Romania, as well as other EU or NATO Member States, is concerned with streamlining the process of military deployment to the eastern flank of Europe so that these forces are ready to fight the war on short notice and respond effectively against potential hostile Russian actions, underscoring the need for a rapid and efficient response.

The development of emerging and disruptive technologies (EDTs) determines, on the one hand, advantages for the evolution and use of the armed forces. On the other hand, they constitute potential dangers as they can become sources of cyberattacks and imply new data security measures. In other words, the technological advance that is prominent in this era of globalization has facilitated the spread of technologies and information, crossing national borders, but has also determined the emergence of new sources of danger and instability, such as the proliferation of weapons of mass destruction, thus generating significant threats to regional or even global security (Frankova, 2023).

Artificial intelligence, the most widespread form of EDTs, continues to make revolutionary progress. In the future, this technology could surpass human abilities. Multiple domains, such as transportation, research, or education, will evolve based on the premise of the „Internet of Things (IoT). In the military field, if the states continue to prioritize their individual security needs and neglect the demands of joint guarantee, developing intelligent military systems that cannot be used in a transnational framework, the risk of rapid escalation of conflicts and the emergence of crises between major powers could intensify.

Emerging and disruptive technologies can shape the new security environment, from the economic and military balance between states to the future of work, wealth, and inequalities within them (Cîrciumaru et al, 2021). These new technologies will produce significant changes in the evolution of international relations and the security situation. In the future, power and dominance will belong to those states that will obtain supremacy in this field. The impact of these technologies will be decisive for

redefining military strategies and doctrines and adapting the concepts of operations, including the deployment of military troops from one place to another.

This article aims to analyse the implications of new types of EDTs in the deployment process and to also highlight how the movement of military forces from one point to another has improved since these new systems and other technology elements were adopted.

The author intends to offer some suggestions for simplifying the deployment process further and ensuring the protection of forces based on the constant evolution of new technologies that influence all fields, including the military one.

The research analyses an essential number of bibliographic sources in the field, such as articles and scientific publications issued in journals with a high impact factor, books, military documents and regulations, online available information, and communiques of accredited institutions of interest in this topic.

By carrying out this research, the author aims to identify the answers to the following research questions:

1. What emerging and disruptive technologies are used in the deployment process?

2. How has the use of these technologies influenced the deployment process?

3. What are the directions towards which the deployment process is heading by using EDTs?

To identify the answers to these questions, the author will follow a subsequent trajectory: performing a brief analysis of the current and foreseeable operating environment, identifying general and specific information on emerging and disruptive technologies, especially those used in the deployment process, and pinpointing their role in this process. Subsequently, the author will highlight potential courses of action regarding the evolution of the deployment process. The primary research method used to conduct this study is documentary analysis.

However, it should be borne in mind that the author may encounter difficulties in carrying out the research and may identify certain limitations. The study's novelty may also determine a limited number of scientific sources from which to obtain information. Additionally, the predominantly military nature of the topic may restrict access to classified information, which would have helped conduct a more thorough investigation.

The article is structured in three chapters. In the first one, the author presents the current and foreseeable operating environment from the perspective of the evolution of EDTs. In the second chapter, there are presented conceptual information regarding EDTs and their role in military deployment. The final chapter highlights the answers to the research questions, focusing on the main EDTs and on their use for military transport and mobility.

1. Delimitation of the Current and Foreseeable Operating Environment

The world is facing new challenges and threats. At the European level, tensions are increasing, and globally, national vulnerabilities, whether economic, environmental, or technological, are increasingly turning into threats that quickly spread in the international environment. It has become evident that peace and security are no longer guaranteed de facto, and dangers that can affect Europe transcend national borders.

If not properly used, new technologies can affect the future security environment. Hence, there is a need to secure the data and information from IT systems in public institutions and, more importantly, to ensure security. Hostile entities can exploit potential vulnerabilities, and interdependent infrastructures can be compromised, irreversibly affecting national security (Cîrciumaru et al, 2021).

After almost three decades of neglecting the military situation in Europe, the Russian invasion of Ukraine highlighted the need to modernize and equip the Armed Forces of European states. The conflict, which began on February 24, 2022, emphasized the need for extraordinary efforts to return and revive military forces in the transatlantic area.

There have been signs of military preparations for a potential conflict since 2014, when Russia annexed Crimea and conducted the Hybrid War against Ukraine. Even before that moment, at the NATO level, troops were increasingly involved in military activities conducted in an assembled multinational environment of a lower intensity. Today, it is clear that NATO and the EU can provide Europe with a credible military force to face any strategic competition only through joint efforts.

Throughout this period, European nations had expeditionary forces in theatres of operations in Afghanistan, Iraq, the Western Balkans or states in Africa. Those military structures were better prepared to operate based on an expeditionary model in stability and support operations outside Europe and less ready to defend their own territory (Tenenbaum & Peria-Peigne, 2023). For these reasons, the military leaders were much better prepared to implement the deployment process in the previously mentioned regions according to the expeditionary model. However, they had yet to study the possibility of developing deployment plans in the European space, mainly towards the eastern flank, that could be applied in a far volatile environment if the moment comes.

Considering the challenges of recent years, more and more countries, especially those in Eastern Europe, have made significant efforts and increased the budget from the Gross Domestic Product (GDP) allocated to defence to a minimum of 2%, for investments in new technologies, armaments, and autonomous vehicles. The latest technological breakthroughs in the general field of artificial intelligence (AI) will come with profound changes in all fields, including the military. Thus, emerging and

disruptive technologies could influence how military actions are conducted or even the fate of war.

As previously mentioned, EDTs can revolutionize the nature of conflicts. One by one, European states began recognizing the importance of EDTs and launched various initiatives for development and research. Globally, EDTs for military purposes are being developed, notably by China, Russia, and the USA (Clapp, 2022). Their progress will impact the evolution of interstate relations, lead to changes in geostrategic relations, and alter power dynamics swiftly. Given these transformations, the current environment appears increasingly unpredictable, intensifying the race to modernize forces and develop effective combat equipment and vehicles.

2. Conceptual Description of Emerging and Disruptive Technologies

In this approach, it is necessary to make a reliable delimitation and understand the two concepts, emerging and disruptive technologies, and their implications on the deployment process and military actions in general.

Emerging technologies are broadly considered innovative technologies that have been recently developed, they are being developed or will be developed in the coming years, and their "development, practical applications or both are still largely unrealized, so that they become figuratively standing out from a background of non-existence or obscurity" (Udrescu & Siteanu, 2021). The range of emerging technologies, such as cloud, innovative computing, artificial intelligence, 5G, robotics, and IoT stands out. In this respect, NATO identifies seven critical emerging technologies in its Emerging and Disruptive Technologies Roadmap: Artificial Intelligence (AI), machine learning (ML), big data (BDA), autonomy, hypersonic, space technologies, quantum computing, and biotechnologies (NATO, 2020).

Although both are part of the new technologies category and have common elements, the emerging ones differ from **the disruptive** in the sense that the second category constitutes "those innovations that create a new market and new financial value, replacing consecrated firms, products, and alliances" (Tăbleț, 2021). The European Defense Fund defines disruptive technologies as "an enhanced or completely new technology that brings about a radical change, including a paradigm shift in the concept and conduct of defence affairs such as by replacing existing defence technologies or rendering them obsolete". (Clapp, 2022).

For a better understanding of these concepts, from a military perspective, in *Emerging Technology Trends for Defense and Security,* emerging technologies are defined as "technologies with low maturity or technology readiness level, currently in development." On the other hand, in the same report, disruptive technologies are considered as "technology convergence that involves merging of existing technologies in order to create new and better possibilities and allows development

and maturation" (Andas, 2020). Regarding this type of technologies, in the same NATO's *Emerging and Disruptive Technologies Roadmap,* we identify the following classification: Big Data, Artificial Intelligence, Robotics, space and bio technology, and hypersonic weapons (NATO, 2020)

Technologies based on artificial intelligence are rapidly evolving worldwide and are used, for example, to optimize some analytical processes or, in the field of transport, to monitor traffic jams. The advance of AI has been driven by the increase of informational capabilities and new algorithms, but also by the availability of data obtained from accessible sources (Academia Națională de Informații "Mihai Viteazul", 2022).

The world is continuously developing, and so is the military environment. To continue this process, advancing military deployment and mobility is necessary. Emerging and disruptive technologies are being integrated to enhance force deployment capability and have become game-changers in the force sustainability, agility, mobility and protection.

3. The Role of Emerging and Disruptive Technologies in the Military Deployment Process

The deployment process is closely related to force protection and military mobility. The latter is an element that analyzes the optimization of route planning and the movement of personnel and materials in much more detail. When military movement is organized, several factors are considered, such as port analysis, position of bridges along routes, tunnels, weather conditions, force protection, or cyber considerations. At the European level, the military transport infrastructure is related to the civil network – Trans-European Transport Network (TEN-T), which provides the needs for the movement of military equipment, vehicles, and personnel on its corridors, in a percentage of 94%, anywhere in Europe. However, considering that this transport infrastructure is civilian, used both in peacetime and in times of conflict, there are risks that it will be exposed to hostile actions. Critical infrastructure depends on new technologies that control and monitor transportation through devices and processes (Administrația Prezidențială, 2020). With these aspects in mind, cyber security is integral to the deployment planning process. Digital systems for military mobility, such as Logistics Functional Area Service (LOGFAS) and automated control systems for aircraft, ships, or trains, are essential for the protection of military transports and for maintaining their records.

The EU has foreseen the need to use EDTs in the process of developing military mobility, including in the *Action Plan on military mobility 2.0*, adopted in 2022 for a period of 4 years. The organization tries, through this plan, to stimulate the development of technologies that improve the field of military mobility. For

example, it advances measures to digitize military transport activities, through the development of secure and quick digital systems through which to ensure the exchange of information, based on AI-type ETDs. Also, it follows the implementation of space-based navigation (Galileo/ EGNOS) secured communication and Earth Observation (Copernicus) that have the potential to significantly benefit military mobility (European Commission, 2022).

The dependence of the deployment process on EDTs refers not only to the development of means of transport and their adaptation to current conditions but also to the securing of transports, monitoring of convoys, transport infrastructure, and digitization of the field. For the deployment process to be effective, the states involved must improve their infrastructure and joint capabilities and use new digital technologies for infrastructure monitoring and logistics planning (European Parliament, 2020). Through the new tool based on EDTs – Information Sharing and Analysis Centers (ISACs), civil-military structures can preserve and subsequently promote information on transports, and critical infrastructure operators can protect their facilities, personnel, and users from physical security and cyber threats (Uniunea Europeană, 2019).

Force protection during the deployment operation is an essential element to be considered, and the new emerging and disruptive technologies bring new solutions for better conditions for an integrated equipment, vehicles, and personnel protection while on the move. Adversaries may employ cyberspace attacks to inflict power outages at home stations, sabotage and target transportation networks to delay shipment of unit equipment, conduct social media attacks, or instigate protests that lower popular support for the Armed Forces (Headquarters, Department of the Army, 2022). Most force protection measures developed recently due to the unprecedented evolution of the concept of EDTs and used during the deployment process are physical measures. In the Romanian Armed Forces Doctrine for Operations, there are 19 measures for force protection, including physical measures (such as security, engineering, EOD, camouflage, Air Defence, CBRN, fire fight, medical, health and environmental), as well as psychological (countering PsyOps, PR, judicial and religious assistance) and electronic (INFOSEC, electromagnetic) ones. Some of the most important measures of force protection regarding the mobility are sensors, automatic barriers, and other remote-control devices to observe enemy activity and prevent possible problems during transportation. These systems can identify dangerous areas and safe transport routes, and the convoy will benefit from the necessary protection. Moreover, new EDTs used in this sense can be operated from a distance, supplementing the level of protection (Ministry of Defence, 2015).

During deployment, several force protection measures must be taken to avoid potential cyber-attacks on convoys or hubs where troops store their equipment, weapons, or ammunition. To achieve this, automating systems and digitizing force

deployment processes are necessary. The new technologies also used in the military field produce a quick reaction in case of an incident by installing programmable logic controllers (PLC) (Stanciu & Gimiga, 2023).

The Ukrainian conflict just highlighted the increasing use of Unmanned Aerial and Undersea Systems (UAVs and UUSs) which poses real threats to force deployments, especially the use of Maritime ships and infrastructure. These systems cause material damage, by destroying infrastructure and military equipment, but they also lead to human losses. From these considerations, in future military operations it is necessary to equip the means of transportation, regardless of their type, with sensors or special systems that provide early warning of the approach of these dangers or additional physical protection measures, such as the use of thicker armour, camouflage, etc. (Samus, 2024).

In recent years, several systems and programs based on EDTs have been developed to ensure the interconnection, security, and digitization of military transport, regardless of the type of transport. In terms of rail transport, used both for civilian passengers, cargo, and for military transport to secure them and to ensure rapid deployments, technologies such as the Internet of Things or the European Rail Traffic Management System (ERTMS) are currently being used - aiming to establish a standard for communications, signaling, management, and control of rail transport at the European level (European Commission, 2022).

Road transport is indispensable for moving military forces from one point to another. Emerging and disruptive technologies present an opportunity to secure the deployment of troops. For example, they are successfully used to monitor and manage traffic lights and traffic control through sensors so that when a military convoy approaches, they allow it to pass under the best conditions (Beckvard & Zotz, 2021). Regarding the development of sensors, new technologies such as LiDAR, which uses laser pulses to omnidirectional measure distances to objects of any size and successfully navigate on land and in airspace, or *dart-shooting* systems for mounting sensors using arrows or other adherent supports placed by drone (Cîrciumaru et al, 2021) are already implemented or in the testing stage.

EDTs based on radio frequency identification (RFID) are also successfully used to monitor the transport of military equipment, materials, or vehicles (Merluşcă, 2024). Thus, the supply process will be improved, with confirmation that all materials have been delivered and arrived safely at their destination. Most importantly – they were received at the right time. Through RFID technology, information indicating the location and delivery time of materials is updated so that military leaders have a clear and complete idea of the stocks of materials they will receive.

Regarding the development of the navigation systems expanded through EDTs designed to ensure the safety of military transports, we can identify what is included in the Action Plan 2.0 on military mobility as information related to

the secure navigation systems used by the military forces of the European states, Galileo/EGNOS, and Copernicus. The Public Regulated Service (PRS) is the most secure Galileo navigation service suitable for governmental applications. It must be reliable even under crisis circumstances, equivalent to the GPS M-Code. Galileo PRS could benefit military mobility by providing uninterrupted, secure, and accurate Position Navigation and Timing information in contested environments, fulfilling critical operational needs in the theatre of operations, and contributing to informed decision-making and command and control. The European Geostationary Navigation Overlay Service (EGNOS), although not designed to operate in a conflict zone, can offer critical operational benefits for logistics and transport operations. In adverse weather conditions, it can enable secure access to air bases and regional airports that do not have other means (European Commission, 2022).

EDTs also play a crucial role in advancing autonomous systems, which are set to revolutionize the military transport sector. This includes trajectory planning, collision avoidance, assisted assistance, dynamic mission planning (navigation, data collection, adaptive detection environment characterization), and extending the operational duration of unmanned underwater vehicles (Ioniță 2022).

From the perspective of military transports, AI has made an exceptional contribution to simplifying the deployment process and reducing material damages or human losses. Several studies have highlighted that more than 50% of casualties among combatants in contemporary conflicts occur while transporting materials, equipment, fuel, or techniques in operational areas (Cîrciumaru et al, 2021). The emergence of remote control vehicles has led to a reduction in the number of victims. In 2019, at the Fort Bliss military base in Texas, the US military presented the first ten trucks capable of moving in the absence of drivers in a convoy. The new transport method involved a driver for the first truck and driverless trucks for the rest (Lee, 2019). Future deployment plans in all operational environments are varied. The goal is to develop a transport system comprising autonomous land, air, and naval vehicles that operate within the operational area under the control of an optimized, automated command centre.

The US is supported through the Tank Automotive Command (TACOM), which manages the Armed Forces's ground equipment supply chain, in developing vehicles that require low maintenance, have a smaller footprint, are lighter, and can self-diagnose potential failure. The new vehicles that the US Army will use will be lighter, have stronger armour, and consume less fuel, thus reducing fuel needs (Sikes, 2023).

The need to ensure a future military transport has become apparent based on the new EDTs, as their specifications will allow better planning and execution of the deployment process. The use of wireless communications, radar, sophisticated computer-aided video detectors, on-board computers, and navigation systems

to ensure a multimodal and integrated transport concept based on technology are measures based on modern technologies, which will ensure interoperability between services and compatibility with civil traffic management and vehicle dispatch system (Brown, Bennett, & Honea, 2020).

Also, emerging and disruptive technologies help to streamline the field of transport and the movement of military forces across European borders over long distances by launching projects such as TRAWA (for the standardization of the drone detection and avoidance system) or ARTURO advanced radar technology (Rodrigues, 2023). In the same vein, the EU has developed the Secure Digital Military Mobility System (SDMMS), which has an implementation deadline of May 31, 2025, and aims to facilitate and secure the exchange of information between states requesting and approving military transports (ASSETS, 2022).

Also related to the field of EDTs and its influence on deployments is the replacement of military vehicles that use conventional fuel sources with new models that use electric or hybrid technologies. Their role is to streamline and lighten the burden from a logistics perspective but also to reduce the adverse effects on the environment. Considering the need for a more sustainable environment, the military field is forced to adapt, and the idea of using new types of transport vehicles is becoming a reality (NSTXL, 2023).

Comparing civilian and military transportation methods, we see the breadth of innovative solutions adopted by private sector companies to simplify the transportation process based on artificial intelligence, robotic technologies, or other EDT-based systems. In the military field, these robotic systems, which in some places are already implemented and yielding results, would streamline the logistics part of the deployment operation. In this sense, the US, for example, promotes using robots for autonomous transport vehicles, such as the THEMIS (Tracked Hybrid Modular Infrastructure System). The US also imports the idea of technological development by using drones to supply and resupply troops or to monitor military transports (Merlușcă, 2024).

Currently, the US Army uses the Joint Flow Analysis System for Transportation (JFAST) model, which can operate in the joint area, determine transportation requirements, provide analysis on courses of action, and design routes for troops and equipment transportation by sea, land, or air. JFAST is a modern multimodal system capable of rapid no-plan development and plan refinement. Through EDTs, the deployment process has been simplified by implementing identification barcodes, microchips, systems that can provide real-time information about transport, and automated systems to support rapid deployment and movement of cargo by air, sea, or land (Brown, Bennett, & Honea, 2020).

Although the US holds supremacy in the technological field among the NATO Member States, one by one, all the Allies began to be concerned by the development

of this field. Romania, in the *National Strategy in the field of Artificial Intelligence 2024-2027,* highlighted the role of artificial intelligence development in optimal transport evolution. The document aims at "the digitization of road infrastructure, by installing sensors for autonomous vehicles that are guided by communication with these sensors and vehicular ad-hoc networks (VANETs), the digitization of documents used in transport and the promotion of intelligent transport systems" (Ministerul Digitalizării, 2024).

Currently, EDTs are essential tools for force projection and force protection, having a special role in the deployment process, by ensuring the physical protection of the personnel and equipment, the development of faster and quicker transport vehicles, and at the same time, simplifying the process itself, by eliminating bureaucratic barriers, digitizing transport forms, satellite monitoring of convoys or automatic planning of transport routes, depending on certain parameters, through digital applications.

Conclusions

New technologies, especially artificial intelligence, are already producing changes in the security environment, as states are concerned with consolidating technological advances simultaneously with the evolution of current threats.

The main component of emerging and disruptive technologies, namely artificial intelligence, impacts the development of critical infrastructure and defence capabilities. The new systems, applications, programs, and projects based on EDTs support the development of modern capabilities to ensure the control, protection, and connectivity of military transports at the national level and within the security framework of the Alliance in the transatlantic space.

The need for society to rapidly adapt to the new models offered by emerging and disruptive technologies is evident. The rapid evolution of technology strongly impacts both social and military environments. Given the concern for ensuring security, states must first ensure the ability to deploy forces in their areas of operations rapidly.

The emerging and disruptive technologies used in the deployment process refer, on the one hand, to the monitoring of transport through digital networks, intelligent and interconnected systems, applications, or programs, and on the other hand, to the modernization of the vehicles and the transport technique used, through the development autonomous systems, which ensure additional protection for military personnel or transported materials and equipment, as well as environmental sustainability.

By using EDTs, the deployment process is noticeably improved. By replacing outdated vehicles with modern and autonomous ones, travel speeds have increased

considerably, and reaction times have improved. Thus, logistics were provided more quickly, and the operation speeded up. On the other hand, the digitization of systems has reduced bureaucracy and connected all transatlantic states to a shared network of military transports in the operations environment. These advantages of EDTs cannot be contested, and their constant evolution requires the permanent adaptation of the armies to the new requirements through significant investments in the development of modern systems.

Among other things, the benefits of these new technologies include eliminating human losses, as soldiers are less exposed to the actions of the adversary, providing accessibility in different locations positioned in a complex operational environment, and reducing bureaucracy and unnecessary waiting times.

Scrutinizing the deployment process's horizon reveals an increasing reliance on digital networks and intelligent, interconnected systems. If the investments in EDTs continue, the deployment process will be completed in a considerably shorter time. This is a minimum cost that a state can assume to ensure the security of its citizens in times when security is increasingly challenging to achieve and maintain.

EDTs intervene in developing measures regarding the deployment process by implementing specific programs and applications, which ensure the protection and securing of military transports, aspects that could not be regulated before. To improve this process in the future, the author considers the following proposals as being relevant:

- implementation, as fast as possible, of a common database at the transatlantic level for real-time monitoring of all types of military transport, such as the RFID automatic identification method;

- the allocation of considerably larger budgets by NATO Member States for the development of modern military transport capabilities based on new emerging and disruptive technologies;

- the identification, promotion, and transfer of cutting-edge technologies from the civilian sector to the military organization to facilitate and boost the operationalization of the multi-domain operations concept. By identifying, in our case, the leading players in the development of intelligent transport systems or software and, subsequently, achieving cooperation and shared interests for the transfer, adaption, and implementation of these technologies in the military organization, the deployment process and force protection during the movement of forces may have been considerable;

- at national level, for the transport of troops, standard software can be used, e.g. LOGFAS, that is accessible to all military units, to monitor transports, verify the tasks of each structure, and reduce waiting times by eliminating bureaucracy;

- developing protocols or procedures to ensure a whole-of-government approach to the military deployment process between ministries with specific attributions, such

as the Ministry of Digitization, the Ministry of Transport, and the Ministry of Finance, to ensure the rapid development of EDTs that could support the targeted field;

- development by the Ministry of Defense of specific programs aimed at ensuring cyber protection of the databases that contain all the information related to the deployed equipment, materials, and personnel to provide force protection and to eradicate the existing virulent informational, hybrid, or cyber vulnerabilities.

The realm of emerging and disruptive technologies is constantly changing and evolving. More and more modern systems are improving the current activity in civil and military fields. In order to ensure the security and deterrence of the European territory, the military must quickly and optimally implement the new EDTs and adapt to all the changes that may occur. Good cooperation at national and international levels can sustain the development of military mobility and ensure prompt deterrence and defence of the eastern flank. Only by understanding the role of new technologies and adapting the military process to the digital evolution will the deployment process be facilitated, and by using robots, drones, or other military systems for dangerous activities performed during the deployment, the number of potential casualties will be reduced. The force protection will be achieved in better ways than before the EDTs.

There is a substantial interest in developing emerging and disruptive technologies to expand future deterrence and defence capabilities, where technological superiority will matter enormously. This dominance will also reduce the quantitative gap between the opponents' armed forces and the human factor invested on the battlefield. In the matter of force deployment, prototypes of autonomous vehicles, new guiding, monitoring, and validation systems, and digital databases that gauge military transports are part of this technological expansion, which influences all domains.

BIBLIOGRAPHY:

Administrația Prezidențială. (2020). *Strategia națională de apărare a țării pentru perioada 2020-2024.* București: Monitorul Oficial, partea 1, nr. 574.

Andas, H. (2020). *Emerging technology trends for defence and security.* Kjeller: Norwegian Defence Research Establishment.

ASSETS. (2022). *ASSETS*. Retrieved from Secure Digital Military Mobility System: https://assets-plus.eu/secure-digital-military-mobility-system/

Beckvard, H., & Zotz, P. (2021). *Cyber considerations for military mobility.* Tallin : NATO cooperative cyber defence centre of excellence.

Brown, S., Bennett, H., & Honea, R. (2020). *US Military Transportation.* Washington: Committee on Military Transportation.

Cîrciumaru, F., & et all. (2021). *Impactul noilor tehnologii asupra artei militare.* București: Editura UNAp "Carol I".

Cîrciumaru, F., Petrescu, D. L., & et all. (2022). *Amenințări și riscuri la adresa securității naționale a României - Orizont 2040.* București: Editura UNAp "Carol I".

Clapp, S. (2022). *Emerging disruptive technologies in defence.* Bruxelles: European Parliamentary Research Service.

European Commission. (2022). *Action plan on military mobility 2.0.* Brussels: European Union.

European Parliament. (2020). *The impact of emerging technologies on the transport system.* Bruxelles: TRAN Committee.

Headquarters, Department of the Army. (2022). *Field Manual FM 3-0- Operations.* Washington: Department of the Army.

Ioniță, C. C. (2022). *Societatea postindustrială și inteligența artificială. Provocări și oportunități din perspectiva securității naționale și a NATO privind dezvoltarea conceptului operației multidomeniu.* București: Editura UNAp "Carol I".

Larsen, H. (2024). *NATO Mobility – It's Tech, Not Just Railroads and Roads.* Washington: Center for European Policy Analysis.

Lee, C. (2019, 02 22). *National Defense*. Retrieved from Autonomous Convoy Tech Moves Toward Official Program: https://www.nationaldefensemagazine.org/articles/2019/2/22/autonomous-convoy-tech-moves-toward-official-program

Merluşcă, A. M. (2024). Digital technologies used in the field of military transport. *Buletinul UNAp "Carol I", no.2 (vol.13)*, 142-150.

Ministerul Digitalizării. (2024). *Strategia națională în domeniul inteligenței artificiale 2024-2027.* București.

Ministry of Defence. (2015). *Allied Joint Doctrine for Force Protection AJP 3.14, Edition A, Version 1.* NATO Standardization Office.

NATO. (2020, 03). *NATO Science and Technology Organization.* Brussels: NATO Science & Technology Organization. Retrieved from NATO Science and Technology Organization.

NSTXL. (2023, 12 22). *National Security Technology Accelerator*. Retrieved from Military Mobility with Hybrid Electric Technologies: https://nstxl.org/military-mobility-with-hybrid-electric-technologies/

Rodrigues, S. (2023). Financing European Defence: The end of budgetary taboos. *European Papers, vol.8, no.3*, 1155-1177.

Samus, M. (2024). Lessons learned from the war in Ukraine. The impact of drones. *New Strategy Center*, 1-28.

Sikes, A. (2023, 07 07). *Department of Defense Manufacturing Technology Program*. Retrieved from the right conversations – TACOM at LIFT Technologies: https://www.dodmantech.mil/News/News-Display/Article/3454403/the-right-conversations-tacom-at-lift-technologies/

Stanciu, C. O., & Gimiga, S. I. (2023). Noile tehnologii şi impactul lor asupra domeniului militar. *Buletinul UNAp "Carol I", nr. 2*, 157-169.

Tăbleţ, R. B. (2021). Integrarea tehnologiilor emergente şi disruptive în arhitectura militară modernă. *INFOSFERA-Revista de studii de securitate şi informaţii pentru apărare, nr. 3*, 73-83.

Tenenbaum, E., & Peria-Peigne, L. (2023). Zeitenwende: The Bundeswehr's paradigm shift. *Focus Strategique, no.116, Etudes de L'IFRI, Security Studies Center*.

Udrescu, M., & Siteanu, E. (2021). Emerging technologies: Innovation, demassification, effectiveness, revolutions in military affairs. *Journal of Land Forces Academy, vol. XXVI, no. 4(104)*, 299-308.

Uniunea Europeană. (2019). *Provocări pentru o politică eficace a UE în domeniul securităţii cibernetice.* Luxemburg: Curtea de Conturi Europeană.

DOI: 10.53477/1842-9904-24-12

MAINTENANCE ASPECTS OF UKRAINIAN DRONES

Petru-Eduart DODU, PhD*

Drones become part of our life, having a huge impact on it. What was beyond our imagination yesterday, becomes true today and will be even better tomorrow. Nowadays, with the help of drones we are able to detect in agriculture the parcels that require herbicides and fertilizer, develop researches in the atmosphere, monitor pollution and dangerous areas, have a better reconnaissance of the domestic infrastructure or obtain an easier victory in conflicts.

The purpose of this paper is to briefly analyze the maintenance required by drone systems - going through a short history of drones, their evolution and classification, their use in the ongoing Russian-Ukrainian conflict as well as the key aspects of their maintenance process. This article aims to provide a concise analysis of the maintenance needs for drone systems. It will cover the drone's brief history, classification and evolution, use in the ongoing Russian-Ukrainian conflict, and important maintenance procedures. Unmanned aerial vehicles have a very small tendency to be maintained in the same way as conventional aircraft (only by qualified aircraft maintenance personnel guided by complete maintenance procedures) due to differences in the personnel, equipment to be maintained, practices, and technical documentation, especially in a combat environment. In fact, untrained operators or maintainers without prior training in aviation maintenance constitute even the staff engaged.

Keywords: *drones; military; maintenance; reliability, operator; unmanned; aircraft.*

Introduction

The expanding selection of drones by a wide set of companies, open administrations and business visionaries guarantees a progressive cost-effective jump forward within the efficiency and execution of businesses, ranging from civilian logistics or infrastructure projects to the military domain. The conceivable outcomes

**** Colonel Engineer Petru-Eduart DODU, PhD, is Deputy Commander within the Romanian Air Forces, Constanța, Romania. E-mail: eduartaero@gmail.com***

for the use of drones can be found today in all divisions of a society. Within the open domain of society drones can be operated for the avoidance of wrongdoing (heat sensors detect unauthorized access on ranches or on border crossings during the night), in countering catastrophes, for governmental civil engineering projects, geographical studies, countering violations of human rights, guarding borders, and for environmental and agriculture assessments. Within the private domain of society there is potential for video surveillance applications (aerial photos and videos), for the assessment and avoidance of neighborhood wrongdoing. There are also various potential applications for drones with different payloads – carrying supplies for helpful purposes or pesticides used in agriculture. Within the military domain, drones are engaged for domestic purposes and in military operations abroad in theaters of operations.

1. A Brief History of Drones

Drones, as defined by the Merriam-Webster dictionary, are uncrewed aircrafts or vessels (performing in air, on water or underwater) guided by remote control or onboard computers. Abbreviations often used when there are topics related to drones are:

− UAVs - Unmanned Aerial Vehicles (used in the industry is the most frequent term, for recreational and professional civilian applications, speeds are quite fast, could reach difficult-to-access areas);

− UAS - Unmanned Aircraft System (describe the entire equipment: the aircraft, the control aparatus and the wireless data link and it is used by American and British organizations as Federal Aviation Administration (FAA – United States), Unmanned Aerial Vehicle Systems Association (UAVSA) – UK and so on);

− RPAS - Remotely Piloted Aircraft System (formal term used by international agencies as the International Civil Aviation Organization (ICAO), the European Aviation Safety Agency (EASA) and so on);

− USV - Uncrewed Surface Vessel is a ship (boat) that performs on the surface of the water not having a crew;

− UUVs - Unmanned Undersea Vehicles (speeds are low, long duration is required but it is affected by high sea currents).

The French language speaking countries use the term “drone” associated with military technology (AltiGator 2024).

The first case recorded in the history of the use of drones (not similar to what is available nowadays in the drone field) was on 1849 in Venice, Italy, during the war for independence when Austrian soldiers attacked the city with approximately 2200 balloons caring small bombs (weighing between 11 kg and 14 kg).

In 1907, brothers Jacques and Louis Bréguet, with the help of French Physiologist Professor Charles Richet, built a gyroplane which was similar to a

modern day quadcopter and performed the first rise of a vertical-flight aircraft which reached a height of 0.6 meters. The flight was not considered a free flight because four men were needed to maintain the aircraft steady during the flight.

In 1916 the first pilotless aircraft named Ruston Proctor Aerial Target was built, serving as a military drone, using a radio guidance system developed by British engineer Archibald Low. The aircraft was launched from the back of a truck using compressed air but later the British military leadership did not follow the path discovered by Archibald Low. It is worth mentioning that very soon an aircraft similar to an aerial torpedo using gyroscopic controls was constructed and it was named Kettering Bug. After the first item the US Air Force produced 50 platforms.

In the 1930 a radio-plane called OQ-2 was developed by British actor Reginald Denny and engineer Walter Righter which later became the first mass-produced drone in the U.S with approximately 15,000 drones being produced.

In 1937 the US Navy Curtiss developed the N2C-2 Drone, a radio-controlled aircraft, and in 1935 the British developed "Queen Bee," a radio-controlled target drone, which is also believed to have led to using the term "drone" for radio-controlled unmanned aircraft.

In WW2 the German Army developed the V-1 "Doodlebugs", the first cruise missile used against London. The equipment used an autopilot for altitude control and airspeed through the force of pressurized air, gyroscopes for yaw and pitch, a magnetic compass for the azimuth and a barometric device for altitude. Afterwards, same capabilities were used by the US who designed the TD2D-1 Katydid and Curtiss KD2C drones.

The Vietnam War (1955-1975) between the communist government of North Vietnam against South Vietnam and its main ally, the United States, witnessed the use of the drones equipped with cameras for reconnaissance and the new purposes for drones in operations such as decoys in combat, launching missiles against fixed targets and the dropping of leaflets against communist propaganda in psychological operations. The Lightning Bugs drone was used in combat missions over North Vietnam and southern China, the flights being controlled by the Strategic Air Command (SAC) from Monkey Mountain Facility in South Vietnam.

Invented in 1947, the transistor technology had a peak in 1960 with its presence inside the drones' mechanisms, especially of the miniaturized radio-controlled components and an increase in radio-controlled planes during the same decade. Thanks to that, planes began to appear in kit form, allowing people to build and fly RC aircraft indoors or outdoors contributing to the development of commercial RC technology.

A drawback in the military domain was considered the price of drones and the lack of trust in the outcome, however, the victory in 1982 of the Israeli Air Force against the Syrian Air Force using drones brought a change in people's minds and a revolution in the use of drones for military purposes (Vyas 2023).

Abraham Karem, born in 1937, is considered today the person who invented the drones. His occupation was designer of fixed and rotary-wing unmanned aircraft and he built his first drone that was used during the Yom Kippur War (between October 6th and 26th, 1973) and from that moment on, the Israeli Air Force began to develop unmanned aerial systems, an example being the presence against the Syrian air fleet jamming communications and providing accurate reconnaissance.

Some milestones to be considered: in 1974 Abe Karem designed the Predator, in 1986 Israel and American military start using the Pioneer, in 1993 monitoring of climate and environment began, in 1999 Predators were used for surveillance and combat in Kosovo, Yugoslavia, Afghanistan and in other conflict areas. In 2007, the Reaper was used in combat missions in Iraq and Afghanistan.

After 2010, we are witnessing an increase in the use of drones as tech toys in non-military fields and an increase of military drone budget, at least in the US, especially under President Barack Obama who ordered a lot more counter-terror strikes than George W Bush (Attard 2024).

2. Drones Classification

Basically, a drone is a flying equipment that can be controlled from a distance or that can fly independently using onboard systems (sensors, a global positioning system, etc.).

There are two types of drones: Rotor type - single-rotor and multi-rotor (such as tricopters, quadcopters, hexacopters and octocopters), and Fixed-wing that could be a regular type and hybrid type with vertical takeoff and landing (abbreviation used is VTOL) –no runways required.

Explicitly, components of a drone are:

- frame (chassis) - the main structure which holds all the parts together;
- motors - fundamental parts that help keep the drone in the air and running;
- drone propellers – comprised by standard propellers and propellers attached to the drone motor making onward movement possible;
- battery - provides power and makes all actions and reactions possible;
- flight controller board - the brain of the drone - responsible for navigation, flight control, communication, etc.;
- electronic speed controller - a device used to control the speed of an electric motor;
- radio transmitter - responsible for the transmission of the radio signals from the controller to the drone to command the flight;
- radio receiver - receives the signal from the drone controller;
- sensors - Position and movement sensors give information about the location of the drone;

– camera - for aerial photography or aerial filming;

– 3 axis gimbal - maintains the drone still and stabilized – a motor is placed on the 3 different axes around the camera);

– GPS - is responsible for providing longitude, latitude and elevation points;

– software-based interface - with the purpose of data collection and analysis using mobile devices or computers;

– software - a collection of algorithms for guidance, navigation and control for autonomous drones or autopilot software used in drone applications;

– remote control - because the use of the radio frequency needed to establish a communication between the remote operator and the drone, remote control signals from the operator's side can be provided from: ground control systems, (a human operating a radio transmitter, smartphone, computer or other similar control systems, remote network systems, (satellite bidirectional communication - can send and receive signals at the same time or wireless data transmission) and another aircraft serving as a mobile control station (relay);

– payload - equipment (even ammunition) able to be carried by the drone to perform a specific mission.

A drone could serve different purposes such as:

– *in the civilian field*: reconnaissance, search and rescue, traffic and weather monitoring, firefighting, personal use drone-based photography and video, and for different services (especially in the logistics domain);

– *in the military field*:

• Intelligence (Signals Intel-SIGINT alludes to data determined from collected electronic transmissions of all sorts, counting catching communications between gadgets such as phones, radios, and computers. Data obtained through SIGINT sensors can be utilized to distinguish, find, and recognize targets for future strikes);

• Surveillance (Wide-Area Surveillance detects military targets within an area of interest thousands of times larger than the coverage of Full Motion Video);

• Reconnaissance – operating at high altitudes with extended endurance (up to 5 hours) covering large areas and collecting high-resolution imagery and data used to identify the location of threats and instantly communicate adequate measures;

• Search and rescue - provide capabilities that are leveraged by emergency situations in an enemy area, operate effectively in various terrains, ranging from dense forests to urban environments;

• Target Practice – drones are used for target practice or for training to develop a better accuracy. The software of a drone able to detect and respond to targets' presence automatically is a real help;

• Force protection – drones carrying explosives are extremely dangerous and effective as weapons and a reliable counter drone system (drone detection, jamming and also kinetic drones capability) are very important to track, identify, mitigate

or destroy hostile drones entering in airspace denied to everyone because ongoing operations;

• Combat (offensive and defensive capabilities), target tracking and acquisition (the method by which a target is identified, recognized, and followed in planning for an accurate strike by another military weaponized platform);

• Buddy lasing – drone's operator points a capable laser label at the target making an impact named "sparkle" and another flying vehicle at that point discharges a laser-guided rocket, bomb);

• Artillery spotting – operations by which an observer located within visual range of a target provides information about the target back to artillery located beyond visual range, also performing fire correction enables actions for adjustment of aim after a first shot);

• Battle damage assessment (because drones are able to fly lower than manned aircraft, used for collecting profitable data amid minimal climate conditions or in profoundly challenged ranges as tactical air reconnaissance to provide information for post-strike analysis and re-strike decisions),

• Communications Relay – a drone provides the link between two or more military manned entities which are not able to communicate with each other directly);

• Electronic attack (EA) (the use of a variety of non-kinetic measures to break apart, degrade, or destroy weapons systems belonging to the enemy);

• Logistics in the military domain – drones can be used for transportation and for contribution in delivering supplies, equipment and ammunition or to evacuate injured military personnel.

In 2020 unarmed drones were more numerous than armed drones according to research by Dan Gettinger in The Drone Databook – 12 out of 95 countries with active military drone inventories confirmed to operate weaponized unmanned aircraft (The U.S., which possessed the biggest inventory, confirmed military operations were more numerous for unarmed drones than armed ones) (Michel 2020).

3. Drones in Ukraine

Because Ukrainians can attack and surveil Russian military troops and equipment using drones, there is a very restricted exchange of technical data concerning them. Using only publicly available data, the following is a brief list of the drones that the Ukrainian military uses:

1. Reconnaissance drones

− Leleka – a Ukrainian-made drone, in service since 2021, speed - 120 km/h, and maximum flight time - 2.5 hours;

− Shark - a Ukrainian reconnaissance drone in service since 2022. It is used for surveillance and fire control, maximum speed - 150 km/h, and the combat radius is 60 km, flight time - 4 hours;

− DJI Mavic-3 – a civilian quadcopter which is the most popular model because of its versatility. Flight time - 46 minutes, maximum altitude - 6 km. Equipped with high-quality optics, it can observe the enemy from above.

2. Reconnaissance drone with thermal imagery

− Mavic-3T – performs surveillance at night, equipped with a thermal equipment.

3. Drones for dropping

− Mavic-3/Mavic-3T – civilian drones, such as the Mavic-3, are equipped with systems for dropping explosives, in trenches or on enemy equipment.

4. Kamikaze drones have a built-in weapon system. They can stay in the air above a target for a period of time and then attack the target at the operator's command.

− Switchblade 300 – an American kamikaze drone with a speed of 160 km/h and flight time of 50 minutes at a distance of 600 meters.

− Pegas – Ukrainian-made drones with a speed of 50-75 km/h, about 400 meters, capable of dropping weapons weighing up to 20 kg.

− First Person View "Goida"" (and related craft names "Bavovna", "Nort Varta") - transmits video in real-time using a camera installed in the front;

− Foxeer – in February 2022 a Ukrainian Foxeer kamikaze drone striked a Russian Grenadier air defence system in Shebekino, Belgorod region, Russia.

− "Falcon Avenger" – an FPV drone transmits video in real-time using a camera installed in the front;

− RAM II – Ukrainian-made strike drone based on the Leleka drone with battle range of 30 km, flight time -1 hour (Molfar 2024).

5. Long Range Attack Drones

− Mugin-5 – available drones such as the Chinese built Mugin-5 (aka Skyeye 5000) - attack the Black Sea Fleet headquarters in Sevastopol, Crimea;

− Tu-143 Reys/Tu-141 Strizh – a Soviet era jet-powered reconnaissance drone still in the inventory of Ukrainian military was weaponized in 2022 and used as cruise missile;

− UJ-22 Airborne – a single engine drone which can either carry an internal warhead or several air-dropped bombs. Payload is up to 20 kg, range - 800 km;

− Morok – carrying a small warhead of 3 kg that has a range of 300 km. It is launched with the aid of a rocket and speed of 290 kmph.

− UJ-25 Skyline – a weaponized development of the Ukrajet UJ-23 Topaz target drone;

− UJ-26 Beaver – has a distinctive canard layout with sleek fuselage and inverted tail. Starting with 2023, it has been built in mass production. It has a range of 1,000 km and payload of 20. This type was used to attack Moscow and other targets in Russia.

− Lyutyy – has resemblance to the Turkish-made Bayraktar TB2 but not in detail.

− AQ-400 Scythe – The Terminal Autonomy AQ-400 Scythe is a volunteer project which has entered serial production. It has a range of max 750 km and payload between than 32 kg and 70 kg (Sutton 2024).

A lot of drones have been reconfigured and upgraded in the last year but the outcome has not been revealed to the public. The President of Ukraine, Volodymyr Zelensky, announced on August 24th in Ukrainska Pravda, an online publication that covers Ukrainian politics, that a new long-range weapon, a combination of missile and drone, called "Palianytsia" after a popular bread brand, had been developed domestically with the intention of striking deep into Russian territory without first requesting authorization from allies to use Western long-range missiles.

Mykhailo Fedorov, Ukraine's minister for digital transformation, told Reuters agency in 2024 that Ukrainian production in 2023 was 300,000 drones and one-third of those were made available to combat forces. Moreover, an additional large number was delivered to the soldiers from different sources.

In regards to the future of Ukrainian drones, we will present some lessons identified. It is obvious that Ukrainians did not obtain an operational or strategic advantage due to the drones utilized in the war because the majority of drones were commercial and the technical characteristics were available to anyone, thus any improvements were known also by the enemy. Even the fact that Ukraine used at first the first-person view (FPV) drones in kamikaze attacks creating do-it-yourself (DIY) cheap kamikaze drones allowed the enemy to quickly adapt to the improvement developing their own type of drones.

Ukraine was the best at utilizing commercial drones in a wartime setting. The Ukrainians were not able to leverage technologies and software advancement to impose the drone supremacy because, at the beginning of the war, the enemy had a large inventory; and, in 2023, the implementation of war production drones domain creates a larger capability on disposal.

Ukraine did not have long-range cruise or ballistic missiles in service and the capability to strike long range targets inside Russia and Crimea was accomplished through drones. Because Russian long-range cruise or ballistic missiles are very expensive, this capability was upgraded with Russian drones trying to surpass the Ukrainian air-defence. In the Ukraine war, both sides have been using counter drone methods. Starting with the end of 2023, Electronic Warfare (EW) has been the most efficient method to block drones through jamming procedures, especially on the path pointing the military area of interest. The use of wire nets as barriers and the attack against drone operators (situated in the proximity of the battlefield) did not provide spectacular results.

Using the artificial intelligence warfare, the Ukrainian drones tried to operate close to the concept of swarms with numerous army units that acted autonomously

and coordinated their operations but in fact the result was a stack behavior with a lot of army operators on the battlefield using traditional means of communication or civilian (commercial) communications platforms.

To sustain the aforementioned opinion, in February 2024, a report from the Center for a New American Security released serious doubts regarding the use of AI in warfare. Stacie Pettyjohn defence program director stated the fact that: "Both parties claim to be using artificial intelligence to improve the drone's ability to hit its target, but likely its use is limited" (Pettyjohn 2024).

Bureaucratic defence procurement system did not allow for sufficient investment to increase the drones production projects. Strong community of Defense Tech foreign stakeholders who benefit from exchanging expertise and opportunities was created to help production and implementation of military technolgy.

Army of Drones project became the driving force behind the UAF's drone activity - 10,000 drone operators received the neccesary training and the aquisition process brought into inventory thousands of drones.

AI should become the next step in improving the identification of the enemy's location more rapidly, determining and transmitting the coordinates to the commander of the striking capability, to make the decision and to destroy the enemy by sending the order to the tool of destruction.

"From the dozens of systems that were in service in early 2022, the Armed Forces of Ukraine used 70 different types of unmanned aerial systems and more than 20 types of ammunition for attack drones at the end of 2023. About 200 companies that manufacture drones in Ukraine produce about 50,000 unmanned aerial systems per month. Plans for 2024 are even more ambitious: to increase the production of FPV drones to 1 million units per year, medium-range attack drones to 10,000 units per year, and long-range attack drones to 1,000 units per year. This number should ensure asymmetric parity with Russia, which is also trying to maximise drone production" (Samus 2024).

In terms of the programs that have driven the UAF's drone activities, one of these programs is the Army of Drones project, part of the national crowdfunding initiative, United 24. Through this project, thousands of drones have been acquired, and over 10,000 drone operators have been trained. Additionally, the United 24 campaign initiated the development of maritime drones, which evolved into a separate state-level program for maritime platforms. Ukraine's advancements in maritime drone technology have significantly impacted the Russian Black Sea Fleet, creating an unexpected strategic situation (Samus 2024).

Despite losing its naval capabilities, Ukraine has successfully used maritime drones to force the Russian Black Sea Fleet to relocate to the eastern Black Sea, avoiding the western areas due to substantial losses inflicted by these drones. Several types of maritime drones have been developed, initially funded by volunteers and later

by the Ministry of Defence and other security and intelligence agencies. Currently, Ukrainian defence forces employ various surface and underwater maritime drones, continually enhancing their features and effectiveness. These drones have inflicted considerable damage on the Russian Black Sea Fleet, its bases, and infrastructure, including the Kerch Bridge. Notably, the Ukrainian drone Magura V522, the primary naval unmanned platform of the Defence Intelligence of Ukraine, sank two landing boats in Chornomorske, Crimea, on November 10, while one was loading a BTR-82, prompting the relocation of the Black Sea Fleet to Novorossiysk (Samus 2024).

In 2023, Ukraine unveiled its first underwater maritime drone, the Marichka. This drone is designed to target ships, bridges, coastal fortifications, and submarines. It can be adapted to carry military or civilian cargo instead of explosives and can also function in a reconnaissance role. The large-scale production of these underwater drones could significantly change the dynamics in the Black Sea, as the Russian Black Sea Fleet may struggle to detect and counter them, posing a substantial threat to Russian warships (Samus 2024).

Additionally, an advanced underwater drone, the Toloka, has been developed with various modifications. The TLK 1000, for instance, has a range of 2,000 kilometers and can carry up to 5,000 kg of explosives. Its guidance system includes passive sonar for identifying and locating underwater and surface objects using hydrophones, as well as ultrasonic (active) sonar for close-range detection, tracking, and object identification by size (Samus 2024).

Organizational and doctrinal changes have also been made, with the Ukrainian Navy creating a naval drone brigade. This brigade is the first naval combat unit of its kind to be equipped with naval drones. These drones are used not only by the Ukrainian Navy but also by the SBU and the Defence Intelligence of Ukraine, working in close coordination at the operational level (Samus 2024).

Russia's war in Ukraine has revealed how important drones are in today's warfare. NATO needs to adapt rapidly. More and higher quality assets are needed regarding drones because the war in Ukraine stressed the fact that "if you haven't invested in sufficient unmanned aircraft capabilities, you're likely to have serious deficiencies against someone who has made the investment" (Federico Borsari and Gordon B. "Skip" Davis 2023).

4. Drones Maintenance Aspects

A drone (military, except kamikaze and civilian), should be kept in proper condition to perform outstandingly and to avoid expensive repairs. There are numerous components that can influence the operability and functionality of a drone such as climate, utilization, capacity, and software overhaul. The main problems could appear on:

− Battery – swelling, leaking, overheating, or losing capacity. To avoid these problems, it is mandatory to utilize the proper charger and to follow the manufacturer's instructions. Also, store the batteries in a cool, dry and ventilated area and check the battery level before and after each flight (it should be changed when signs of wear or damage appear);

− Propeller – propeller damage by collisions, debris, or wear and tear which can reduce the efficiency and stability of the drone causing vibrations, noise, or even crashes. To avoid this problem, the recommendation is to check the propellers before and after each flight to determine the changes in its condition. The propellers should be cleaned periodically (they should be changed when signs of wear or damage appear because they are difficult to repair in an area of operation);

− Motor – responsible for rotating the propellers and controlling the speed and direction can be affected. Unfortunately, they can suffer from issues such as overheating, burning, or jamming. To mitigate these issues, the flights should occur in dust-free environments, to avoid extreme temperatures moderate temperatures are preferred, bearings should be lubricated and the vents should remain clean (they should be changed when signs of wear or damage appear);

− Camera – photos and videos could be affected by poor settings to light or weather conditions or by malfunction caused by gimbals system resulting in distortions of color (lens should be changed when signs of wear or damage appear);

− GPS – errors, such as weak signals, interference, or drift of the Global Positioning System create an impediment for the drone to locate itself and to navigate and return home. These problems are avoided if the flight occurs in open and clear areas with no interference and the drone is in proper technical condition (the firmware is updated), the GPS module and the IMU (inertial measurement unit) calibrated. The operator should also maintain secure flight lines, avoiding power lines, high-rise obstacles and areas with different bodies of water that cause interference with GPS signals;

− Firmware – software that runs on drone when it is updated to improve performance or to add new features could create compatibility problems, which can affect its functionality. To avoid these issues, the manufacturer's instructions should be implemented with accuracy and the drone should be checked after each update first in a secure area, close to the operator (Vineeth Jacob Anthony n.d.).

The primary distinction between maintaining a conventional aircraft and an unmanned aerial system that the UAS technician is accountable for the entire system, which includes the flying apparatus and a variety of ground-based apparatus (a new set of requirements specific to UAS maintenance is introduced by maintaining ground-based components, desktop and laptop computers are now considered airworthy products). The technician must not only make sure that every component of the system is operating as intended, but also that the links connecting the various systems are operating as intended.

Drone systems, military or civilian, require almost the same logistics support as most manned aircraft including the unmanned aircraft and the ground control station. Research and development has an objective to design a system with a reduced logistical footprint, characterized by fast deployment and high mobility with a reasonable maintenance program. Because drones are more and more complex and composed by many sub-systems which perform in the same time it is more difficult to maintain a large drone fleet without a *Maintenance Program*. To provide more safety and confidence to drone operators (to fulfill the mission) there are available *Maintenance Programs* composed of three types of adaptive maintenance (according to the daily flight hours and environment of action) and a recommended maintenance cycle.

In the most basic terms, drone maintenance is the act of inspecting, mending, and replacing any malfunctioning components and generally speaking, there are three primary types of maintenance: preventative, ongoing, and emergency. The kind of drone maintenance that should constantly be performed is the preventative one since it keeps minor problems from becoming major ones – long-term maintenance costs are decreased, and the operator is confident that the drone will operate constantly in the air. In terms of expenses and downtime, ongoing maintenance is comparable to preventative maintenance – even though there might not be a problem with the drone, it is still advisable to carry out the maintenance after a number of flight hours to make sure all the components are in good operating order. After a component breaks down or the drone malfunctions in some other way, emergency maintenance is necessary, but it usually is more expensive and takes longer than preventative maintenance (Spires 2021).

The controller of the drone should respect the user manual regarding the maintenance regime:

− the pre-flight and post-flight inspections are mandatory;

− Operational (Basic) Maintenance: includes changing propellers, carrying out firmware updates and test flights, and calibrations, etc., which will be recorded in the maintenance logbooks;

− Intermediate (Routine) Maintenance: a more detailed inspection or repair will be performed by producer technical personnel when local maintainers are not authorized – it could include components replacement because wear and tear;

− Depot-Level Maintenance: maintenance beyond the capabilities and/or facilities of the field will also consist in verifying the Line Replaceable Unit malfunction, isolation and repair of part(s). Activities could require overhaul, upgrading, or rebuilding of parts, assemblies, or subassemblies and could include the replacement of propulsion system (Vachtsevanos 2015).

Although it may seem tedious, drone maintenance keeps them operating longer and guarantees safe, effective (for the intended purpose) flights. Regular inspections and prompt replacement of broken components stop additional deterioration and

reduce the need for expensive repairs or component replacements. Over time, preventive maintenance reduces costs – by reducing the likelihood of catastrophic failures, preventive measures and early problem detection can save money on repairs and downtime when operational needs are paramount. Tracking a drone's long-term history may lose significance if the most important system components, such as wings or engines, are replaced but real-time data and sophisticated analytics are essential for predictive maintenance - drone component performances and conditions monitoring allow for the early detection of faults before they happen. Algorithms evaluate the data collected by sensors and diagnostic instruments to forecast when maintenance needs to be done for maximizing drone availability while reducing unnecessary servicing. Data management is critical to the effectiveness of operations because it helps with maintenance planning, informed decision-making, and performance insights that enable operators to foresee and avert possible problems. The integration of technologies not only improves overall drone fleet reliability but also streamlines operations and considerably lowers maintenance expenses.

The maintenance teams are composed of multiskilled personnel; they do all the ground work, including assembly, flight planning, and in-flight operations (small drones often have a single owner or operator who handles all maintenance and other duties). Within the military drone domain, there is typically a two-tier system that distinguishes between major repairs and routine operating maintenance. Simple preventative maintenance, refueling, servicing, daily inspections, and replacing line-replaceable units are all included in basic operational maintenance performed by military personnel and structural repairs, overhauls, and the diagnosis and correction of complex faults - major repairs are the responsibility of the manufacturer personnel.

Logistic support elements could be described by:

− primary systems characteristics: reliability, availability, maintainability and safety;

− support system elements: maintenance, training, spares, tools, transport, availability of technical publications.

R.A.M.S. refers to "Reliability, Availability, Maintainability, and Safety". Reliability, availability, maintainability and safety are connected together, but a drone could not be available not only because unfinished maintenance, but also because of different causes. The availability of a drone is a measured probability that the drone would not fail or it would not undergo a maintenance action when it needs to be used. In the field of maintenance, availability depends on maintainability, on the maintenance organization capability (sizing, skills of maintenance personnel, availability of technical documentation, tools used, amount of spare parts available). It is important to not forget that Integrated Logistic Support requests that the logistic support system has to be designed at the same time with the design of the primary system in order to not have future problems of compatibility and to obtain efficiency.

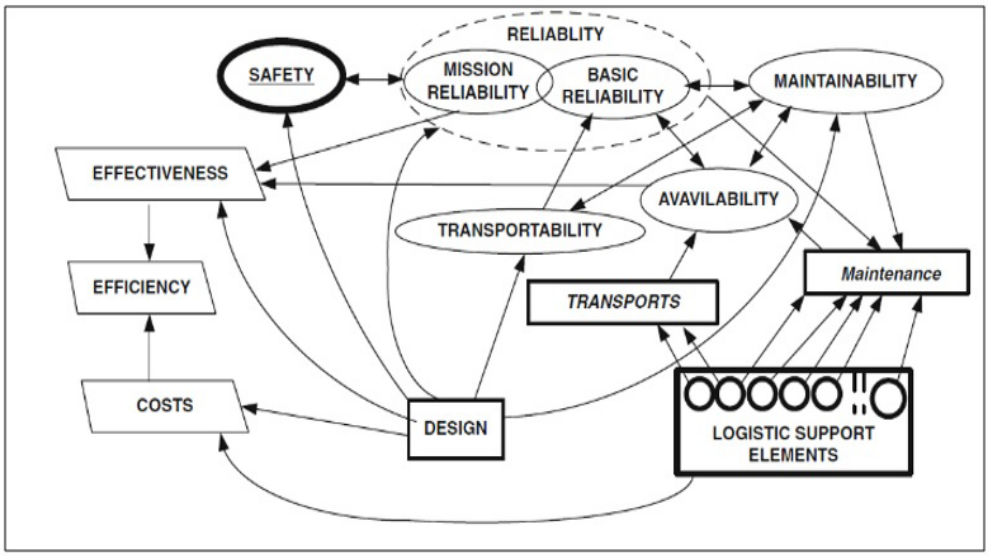


Figure no. 1: Relationship between R.A.M.S., logistic support elements, design and other related issues (Vachtsevanos 2015)

The values of safety, reliability and maintainability are obtained by the design of the product itself. Maintainability, the probability that a failed technical system will be restored to a specified condition in a specified period of time when maintenance is performed in accordance with the producer procedure imposes automatic diagnostics. Reliability deals with the risk of failures in an equipment focusing on equipment availability, performing the task, and the cost involved.

The commercial aviation failure rate is about 1/105 flight hours, while for commercial (civilian) drones, it has been identified at about 1/103 flight hours (Enrico Petritoli 2018).

Even in the case of drones, it is necessary to define the criteria for the level of reliability:

− catastrophic failures: a crash of the drone;

− severe failures: heavy damages to the drone – the probability of being in service again is very low or it requires high costs in the adjacent area of production costs;

− moderate failures: a moderate degradation of the drone's functions could lead to abortion of mission;

− soft failures: light degradation of the drone's functions, does not request to abort the mission.

Commercial Drone (a)			
System Description	λp System FIT (F/10⁶ hrs)	MTBF (hours)	Incidence (%)
Ground Control System	2.00	500,000.0	6.62%
Mainframe	2.77	360,984.8	9.16%
Power plant	9.94	100,603.6	32.88%
Navigation system	9.41	106,269.9	31.13%
Electronic system	5.01	199,600.8	16.57%
Payload	1.10	909,090.9	3.64%
λ TOTAL =	30.23	FIT	
MTBF (R_{Total}) =	33,079.50	Hours	
	1378.31	Days	
	49.23	Months	
Military Drone (b)			
System Description	λp System FIT (F/10⁶ hrs)	MTBF (hours)	Incidence (%)
Ground Control System	14.00	71,403.6	27.30%
Mainframe	2.77	360,984.8	5.40%
Power plant	21.08	47,428.7	41.10%
Navigation system	7.39	135,369.3	14.40%
Electronic system	3.44	290,942.9	6.70%
Payload	2.62	382,219.2	5.10%
λ TOTAL =	51.30	FIT	
MTBF (R_{Total}) =	19,493.18	Hours	
	812.22	Days	
	29.01	Months	

Figure no. 2: Comparison between the reliability of a commercial and a military drone (Enrico Petritoli 2018)

Due to its complexity, a military drone is inferior in terms of reliability to a commercial drone – MTBF (the average time between failures of a system) is smaller to military drones.

In 2022 the lifespan of military drones on the battlefield depended on the type of design:

− a fixed-wing drone lasted for about six flights;

− a rotary-wing drone (quadcopter) lasted for three flights (www.technology.org 2022).

Conclusions

The evolution and diverse applications of drones have revolutionized various sectors, ranging from civilian logistics and environmental assessments to military operations. The parts of a drone are occasionally put back together and taken apart before and after each flight in the battlefield areas. Regularly connecting and disconnecting electrical and other systems might raise the risk of malfunctions, damage and factors such as weariness, bad illumination, and the operating environment can all increase the likelihood of error but it underlines the need of trained and professional maintainers. The maintenance staff should be proficient in

using a variety of technologies, such as computer software and hardware, autopilots, radio communication equipment, modems, and radio frequency interference dangers, in order to connect with and control the drone (very challenging to define in detail the skill and knowledge requirements for maintenance professionals in the small drone area due to its diversity and fast rate of change). In military operations the operating crew need the abilities and expertise required to comprehend how components work together, diagnose small malfunctions, and connect system aspects.

Maintenance of drones is crucial to ensure their optimal performance and longevity. Proper care of components such as batteries, propellers, motors, and cameras is essential to avoid malfunctions and costly repairs. The integration of advanced software and GPS technology further enhances the operational efficiency of drones. Military drones, in particular, require rigorous maintenance protocols and logistic support to maintain their reliability and effectiveness in various combat scenarios. Preventive maintenance is a key component in reducing drone maintenance expenses – frequent inspections and maintenance assist in identifying problems before they worsen and help save costly repairs. Human error and further expenses are decreased by automating maintenance inspections with software tools and on-board diagnostics. Purchasing affordable technology, drones with sophisticated sensors for self-surveillance can give real-time data and support predictive maintenance. This data-driven strategy guarantees effective resource allocation, further reducing expenses. By ensuring that operators and maintenance personnel are proficient in doing minor repairs and maintenance, training programs help to minimize downtime and reliance on professional technicians. Working together with outside maintenance companies can be advantageous as well, since they can provide resources and experience that are not always available inside.

The absence of repair facilities and issues with the supply chains that affect the scarcity of spare parts on the battlefield or in the surrounding areas have a significant impact on the entire maintenance process, which could become too sluggish to be viable. Waiting times for maintenance activities may increase due to logistical factors such as the location of spare parts remote from operating activities in Ukraine or overseas. These factors could be mitigated with effective management and local maintenance solutions.

In the context of the Ukraine conflict, drones have played a significant role, demonstrating both their potential and limitations in warfare. Ukrainian forces have utilized a range of drones for reconnaissance, combat, and logistical purposes. Despite the initial advantage, the widespread availability of commercial drone technology has allowed adversaries to quickly adapt and counter these capabilities. The use of drones for long-range strikes and maritime operations has provided strategic advantages, thus the effectiveness of counter drones measures like electronic warfare has highlighted the ongoing technological arms race.

Looking forward, the future of drone technology in Ukraine and beyond will likely hinge on advancements in artificial intelligence, improved maintenance practices, and strategic innovations in drone deployment. The lessons learned from the Ukrainian experience underline the importance of continuous development and adaptation to maintain a tactical edge. As drone technology evolves, its impact on both civilian and military domains will continue to expand, driven by innovation and strategic application.

BIBLIOGRAPHY:

AltiGator. 2024. *Drone, UAV, UAS, RPA or RPAS.* Access 22. August 2024. https://altigator.com/en/drone-uav-uas-rpa-or-rpas/

Attard, David. 2024. *The History of Drones: a wonderful, fascinating story over 235+ years.* 25. April. https://www.dronesbuy.net/history-of-drones/

Enrico Petritoli, Fabio Leccese, and Lorenzo Ciani. 2018. «Reliability and Maintenance Analysis of Unmanned Aerial Vehicles.» *New Sensors for Metrology for Aerospace* 3. Access 25. April 2024. https://www.mdpi.com/1424-8220/18/9/3171

Federico Borsari and Gordon B. "Skip" Davis, Jr. 2023. «An Urgent Matter of Drones.» *CEPA.*

Michel, Arthur Holland. 2020. «UNARMED AND DANGEROUS The Lethal Applications of Non-Weaponized Drone.» *Center for the Study of the Drone at Bard College* (Center for the Study of the Drone at Bard College) 1-36.

Molfar. 2024. *Angry Drones of Ukraine Armed Forces. What types of kamikaze drones are most publicly mentioned: statistics and examples.* Access 25. April 2024. https://molfar.com/en/blog/angry-drones-yaki-droni-kamikadze-zsu-naychastishe-zgaduyutsya-v-media-statistika-i-prikladi

Pettyjohn, Stacie. 2024. «Evolution Not Revolution Drone Warfare in Russia's 2022 Invasion of Ukraine.» *Center for American New Security.*

Samus, Mykhailo. 2024. «Lessons learned from the war in Ukraine. The impact of drones.» *New Strategy Center* 1-28.

Spires, Josh. 2021. *spheredrones.com.au.* 22. March. Access 22. August 2024. https://spheredrones.com.au/blogs/news/what-is-drone-maintenance-preventative-ongoing-and-emergency?srsltid=AfmBOopL93ViPit2c3JWkIiCmRbe_wdegryQRxODlrwa_F-scTPAUhzW

Sutton, H.I. 2024. «Guide To Ukraine's Long Range Attack Drones.» 26. April. http://www.hisutton.com/Ukraine-OWA-UAVs.html

Vachtsevanos, Kimon P. Valavanis George J. 2015. *Handbook of Unmanned Aerial Vehicles.* Springer.

Vineeth Jacob Anthony, Ryan Bowser, Nnaemeka Obayi. n.d. *What are the most common UAV maintenance issues?* Access 25. April 2024. https://www.linkedin.com/advice/1/what-most-common-uav-maintenance-issues-skills-drones-vixpf

Vyas, Kashyap. 2023. *A brief history of drones: from pilotless balloons to roaming killers.* 18. April. Access 25. April 2024. https://interestingengineering.com/innovation/a-brief-history-of-drones-the-remote-controlled-unmanned-aerial-vehicles-uavs

n.d. *What is an average lifespan of a military drone in Ukraine?* Access 25. April 2024. https://www.technology.org/2022/12/01/what-is-an-average-lifespan-of-a-military-drone-in-ukraine/

www.technology.org. 2022. *What is an average lifespan of a military drone in Ukraine?* 01. December. Access 25. April 2024. https://www.technology.org/2022/12/01/what-is-an-average-lifespan-of-a-military-drone-in-ukraine/

DOI: 10.53477/1842-9904-24-13

VALIDATION AND PRIORITIZATION OF KNOWLEDGE, SKILLS AND ABILITIES FOR CYBERINTELLIGENCE ANALYSIS IN INTELLIGENCE AND NATIONAL SECURITY

Cristian CONDRUȚ*

Cybersecurity educational endeavours are nowadays of interest to public and private institutions as proven by the fact that multiple academic and training formats are available in academia and professional organizations. Given that cyberintelligence developed as a subfield of both intelligence and national security and cybersecurity, education and training are needed to form intelligence analysts that deal with cybersecurity threats in intelligence and national security organizations. Our main objective is to validate and prioritize a set of cybersecurity and intelligence competences that can be used in education and training endeavours for the cyberintelligence analysts in intelligence and national security organizations. Our results show that the high-priority competences for this type of professionals are a mix between intelligence and cybersecurity competences, most prevalent being the analytical and contextual dependent ones. In our article, we also elaborate on examples of educational practices that can be applied to high priority competences.

Keywords*: cyberintelligence analysis; intelligence analysis; national security; competences; knowledge; skills; abilities; education.*

**** Cristian CONDRUȚ is a PhD Candidate at the Doctoral School of Intelligence and Security within "Mihai Viteazul" National Intelligence Academy, Romania. He holds a MSc in Theory of Information Encoding and Storage at Politehnica Bucharest University, Bucharest. E-mail: condrut.cristian@animv.eu***

Introduction

Nowadays, most formal and informal educational endeavours begin with a proper process of identification and development of competences. One of the principles that underpins the definition of competence is that it involves applying contextually-appropriate knowledge and skills (Vitello, Greatorex and Shaw 2021, pp. 15 - 16). Thus, given that cyberintelligence analysis is still a novel field in cybersecurity and in intelligence and national security, in which the diversity and complexity of cyber threat actors are quite high, it is really important to train future professionals by using educational programs that are well-calibrated and adjusted to their purposes.

In our particular research context, which is cyberintelligence analysis in intelligence and national security, it is important to capitalize on previous cybersecurity and intelligence and national security expertise. Borum and Sanders in *Preparing America's Cyber Intelligence Workforce* presented 5 types of competences needed by the cyberintelligence analyst: technical, knowledge management, analytical, contextual, and communicational and organizational (Borum and Sanders 2020, 67-73). In our previous researches, we clustered knowledge, skills and abilities retrieved from the Workforce Framework for Cybersecurity (NICE framework), which was elaborated by the US National Institute of Standards and Technology (NIST), into the aforementioned types of cyberintelligence competences developed by Borum and Sanders (Condruț 2023). Thus, we identified 51 knowledge units, 28 skills and eight abilities necessary for the cyberintelligence analyst in intelligence and national security (Condruț 2023, 4205 - 4206). Given that our previous researches is based only on secondary data (i.e., employing a content analysis methodology on analytical cybersecurity reports), the following research question will guide our endeavour towards a more empirical approach that will involve the employment of research methods needed for the collection of primary data: *How can we validate and prioritize knowledge, skills and abilities needed by the cyberintelligence analyst in intelligence and national security?*

Thus, our research objective is to validate and prioritize the set of competencies retrieved in our previous researches by applying a survey with the participation of cybersecurity, cyberintelligence and intelligence and national security experts. We consider that validation of our previously discovered set could be satisfactory for research purposes, but the prioritization of these competences is necessary for research and educational purposes, given the limited human, financial and logistical resources that could be employed in an educational setting.

In order to test de validity of a more comprehensive set of competencies, we proposed to add eight more knowledge units presented by Alsmadi in *The NICE Cyber Security Framework. Cyber Security Intelligence and Analytics Second Edition*

(Alsmadi 2023) that refer to intelligence analysis and dissemination processes and emergent technology knowledge, thus capitalizing not only on cybersecurity, but also on intelligence analysis. We will present the complete set of competences in the *Methodology* section.

1. Methodology

As stated in the introduction, we applied the survey research method. Thus, our research includes a data collection stage and a data processing stage. In the collection stage we applied a mixed questionnaire (i.e., both with closed and open questions) to cybersecurity, cyberintelligence and intelligence and national security experts from organizations that deal directly with cyberintelligence or that are at the nexus of the tree aforementioned professional domains.

We chose to sample the organization from whom we aim to retrieve answers by using the judgmental sampling procedure (Sharma 2017, 751 - 752), given the fact that we aimed at collecting opinions from intelligence and national security professionals that work in organizations which do not disclose their number of employees in public sources. We selected public and private organizations that have legal responsibilities, commercial, educational or research interests in cyberintelligence, cybersecurity or in intelligence and national security. Thus, we distributed the questionnaire to experts associated with Intelligence College in Europe, International Association for Intelligence Education, NATO Cooperative Cyber Defence Centre of Excellence, European Union Agency for Cybersecurity, Romanian National Cyber Security Directorate, National Institute for Research & Development in Informatics - ICI Bucharest, Romanian Association for Information Security Assurance, Rey Juan Carlos University from Madrid, National University for Science and Technology Politehnica București and Recorded Future.

The questionnaire used included a total of 95 knowledge units (i.e. 59), skills (i.e. 28) and abilities (i.e. 8)[1], each of them being a separate variable and is organized into four sections that contains both closed and open questions: 1) knowledge units; 2) skills; 3) abilities; 4) demographics. For the first three sections, the participants are asked to evaluate on a 6-point Likert scale the importance of each knowledge

[1] Given that the 95 competences are a part of our doctoral research, the main list, consisting of 87 competences, can be consulted in the First Scientific Report, "Cunoștințe, abilități și aptitudini de securitate cibernetică derivate din interacțiunea dintre securitate cibernetică în intelligence" [Cybersecurity Knowledge, Skills and Abilities Derived from the Interaction Between Cybersecurity and Intelligence], library code REF.18, and the 8 additional competences presented in the Introduction, can be consulted in the Second Scientific Report, "Proiectarea instrumentului de evaluare a competențelor prioritare de analiză de cyberintelligence în domeniul intelligence și securitate națională" [Designing a Pedagogical Assessment Instrument for Cyberintelligence Analysis High Priority Competences in Intelligence and National Security], available at "Mihai Viteazul" National Intelligence Academy Library, library code REF.22.

unit, skill and ability. After each of the first three sections, participants are asked to provide any missing elements and arguments. In the last section, demographics, participants are asked to provide their gender, age, work experience in cyber security or a related field, main work field and geographical location of the current employer. The questionnaire was distributed mostly online, but also on-site, depending on the accessibility of the researcher to the chosen experts. After the questionnaire dissemination and analysis of responses, the collection stage of our research was finished.

In order to ensure the reliability of the collected data, we applied two cumulative criteria: 1) exclusion of all responses generated by respondents who have no experience in cybersecurity or in a related field; 2) exclusion of all responses generated by a respondent that did not answer to all of the closed questions (i.e., this applies only for the on-site distributed questionnaires). In order to statistically analyse the data, we applied a procedure based on frequency analysis, mean and standard deviation for each knowledge unit, skill and ability. The following procedure, and in particular the threshold values, are inspired from Nilsen, that conducted similar research in order to validate and prioritize generic cybersecurity competences for regular users in public and private organizations (Nilsen 2017, p. 5). Our statistical analysis procedure followed two stages, each of them corresponding to validation and, respectively, prioritization of cybersecurity competences for the cyberintelligence analyst in intelligence and national security.

In the first stage of our statistical analysis, we considered a particular competence to be validated only if the sum of the frequency of the superior values on the 6-point Likert scale (i.e., 4, 5 and 6) is equal or above the value obtained by computing 70% of the total valid responses obtained for that particular competence. In the second stage of our statistical analysis, we considered a particular competence to have great priority, only if it respects the following descending criteria in order of importance: 1) standard deviation is less than 1, given the fact that we aim to select only those competences that generated consensus among responders; 2) average is above 5 for the valid responses (i.e., out of a maximum of 6), given the fact that we aim to select only those competences that are very important (i.e., the fifth point on the 6-point Likert scale) or extremely important (i.e., the sixth point on the 6-point Likert scale) for most respondents; 3) the value computed in the first stage of the statistical analysis is above 90%, given that we aim to filter from the validated competences only those that are extremely important for 9 out of 10 respondents.

2. Results

The questionnaire was distributed online, between June and September 2023, via Google Forms, and on-site, by the researcher. We collected a total number of 44 responses and by applying the exclusion criteria presented in the *Methodology*

section, we considered 39 as valid (i.e., 5 of the respondents having no experience in cybersecurity field or in related one). Thus, in Table no. 1 we present the demographic data associated with our valid responses.

Table no. 1: Valid responses

Item	Units of choice	Code	Sum
What gender do you identify as?	male	21	27
	female	22	9
	I would rather not tell	29	3
TOTAL			**39**
How old are you?	18 – 24	31	3
	25 – 29	32	8
	30 – 34	33	7
	35 – 39	34	8
	40 – 44	35	5
	45 – 49	36	1
	50 – 54	37	5
	55 – 59	38	1
	over 60	39	1
TOTAL			**39**
How long have you been working in cybersecurity field or related?	1 – 10 years	41	28
	11 – 20 years	42	6
	over 21 years	43	5
	no experience	49	0
TOTAL			**39**
Which of the following professional fields describe your work experience best?	public administration	51	2
	cybersecurity	52	12
	IT (other than cybersecurity)	53	1
	finance	54	1
	education	55	1
	research	56	1
	legal	57	0
	intelligence / law enforcement / defence	58	21
	other	59	0
TOTAL			**39**
From a geographical perspective, how would describe your organization?	public or private organization from Romania	61	20
	public or private organization from European Union (other than Romania)	62	11
	public or private organization from Europe (other than European Union countries)	63	0
	public or private organization from non-European countries	64	2
	international organization	65	4
	multinational company	66	2
TOTAL			**39**

By applying the first stage procedure of our statistical analysis, we identified that 86 out of the total of 95 analysed competences were validated by respondents (i.e., 91.5% of our set of competences were validated)[2]. We will elaborate on those results in the *Discussions* section of the current article. By applying the second stage procedure of our statistical analysis, we discovered that only 8 competences are following the established quantitative criteria. Thus, in Table no. 2 we present the high priority competences for the cyberintelligence analyst in intelligence and national security. We will also elaborate on this results in the *Discussions* section.

Table no. 2: High priority competences of the cyberintelligence analyst in intelligence and national security

Competence code as stated in Table no. 1	Content of the competence[3*]
K0315	Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing information.
S0229	Skill in identifying cyber threats which may jeopardize organization and/or partner interests.
K0538	Knowledge of target and threat organization structures, critical capabilities, and critical vulnerabilities.
S0212	Skill in disseminating items of highest intelligence value in a timely manner.
K0110	Knowledge of adversarial tactics, techniques, and procedures.
S0359	Skill to use critical thinking to analyse organizational patterns and relationships.
S0210	Skill in developing intelligence reports.
A0084	Ability to evaluate, analyse, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/intelligence products.

3. Discussions[3]

3.1. Clustering validated competences

In order to have a more structured view of the validated competences, we continued our previous research (Condruț 2023, 4206 - 4207) by clustering the validated knowledge, skills and abilities into the five types of cyberintelligence analysis competences proposed by Borum and Sanders (2020). Thus, in Table no. 3, we present how many of the validated competences can be clustered in each of the five types and we compare our current results with our previous ones (2023, pp. 4206 - 4207). We performed our clustering by applying definitions for each type of competences for every validated cyberintelligence analysis knowledge, skill and ability.

[2] The complete results can be consulted in The Second Scientific Report, *"Proiectarea instrumentului de evaluare a competențelor prioritare de analiză de cyberintelligence în domeniul intelligence și securitate națională"* [*Designing a Pedagogical Assessment Instrument for Cyberintelligence Analysis High Priority Competences in Intelligence and National Security*], available at "Mihai Viteazul" National Intelligence Academy Library.

[3] As stated in 2017 version of NICE Framework spreadsheet available at https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-current-versions

Table no. 3: Clustering the validated cyberintelligence knowledge, skills and abilities

Type of competence and definition	No. of knowledge	No. of skills	No. of abilities	Total	% from total no. (*i.e.* 86)[4]	Previous % (Condruț 2023)[4]
Technical Competences – "The technical foundation for understanding the hardware and software of information and communications technology, especially as they relate to cybersecurity." **(Borum and Sanders 2020, 69)**	23	9	3	35	**40,7 (4)**	44,2 (4)
Knowledge Management Competences – "The knowledge management and information science foundation for planning and organizing information collection (collection management), applying tools to gather and support complex data and information analysis and presentation." **(Borum and Sanders 2020, 69)**	14	6	2	22	**25,6 (5)**	22,1 (5)
Analytic Competences – "The human science basis for complex analysis of data and information from a variety of sources, including foundations of strategy, critical and systems thinking, reasoning and logic, problem solving, and decision making." **(Borum and Sanders 2020, 69)**	24	27	8	59	**68,6 (1)**	66,3 (2)
Contextual Domain Competences – "The sector-specific, national/regional, and/or sociocultural foundations for analysing complex problems; identifying key actors and roles; assessing perceptions, interests and intentions; sense making; drawing inferences from actions and behaviours; and discerning situational influences." **(Borum and Sanders 2020, 69)**	25	23	8	56	**65,1 (2)**	67,4 (1)
Communication and Organizational Competences – "These competences emphasize clear expression of opinions and reasoning, along with effective communication of one's ideas in writing, oral presentation, and visual display, as well as project management skills." **(Borum and Sanders 2020, 69)**	19	14	7	40	**46,5 (3)**	45,3 (3)

By comparing our previous cluster analysis results with our current results, we observe that there are some differences between the two hierarchical orders of competences from Table no. 3. Thus, in our hierarchical order, the analytical

[4] We present in brackets the hierarchical order of each type of competence, 1 being the highest and 5 the lowest.

competences (i.e., 68,6%) have a slightly higher percentage than contextual domain competences (i.e., 65,1%), while our previous research hierarchical order, contextual domain competences (i.e., 67,4%) have a slightly higher percentage than analytic competences (i.e., 66,3%). This result could be a consequence of the way the questionnaire sample was built or a consequence of difference knowledge, skills and abilities that were considered in our cluster. Even more interesting is that the cluster percentages can be grouped in approximately three intervals, thus giving us an interpretation regarding the composition of our validated competences set: 1) analytic and contextual domain competences are grouped around 67%, with a deviation of 2%; 2) communication and organizational competences and technical competences can be grouped around 43% value with a deviation of maximum 2.5%; 3) knowledge competences scored 25.6% and cannot be grouped with other types of competences. This result shows us that analytic and contextual domain competences are the most prevalent in our validated set of competences, meaning that the cyberintelligence analyst should be more oriented towards knowledge, skills and abilities that are associated with the intelligence and national security domain, rather than with the technical ones. This inference is completed by the results associated with the second and the third interval, given the fact that technical and knowledge management competences are the least prevalent in our validated competences set. Thus, we assess that the cyberintelligence analyst should possess competences oriented towards intelligence analysis, applied to particular security contexts and general understanding of technical concepts. Also, it is important to note that in the second interval, we find the communication and organizational competences. This suggests the fact that the cyberintelligence analyst in intelligence and national security organizations has to be aware and apply internal regulation, protocols and norms and, in general, be adapted to the particularities of the organizational culture from these organizations.

3.2. Development of high priority competences

As previously stated, our research intention is to prioritize the validated competences in order to serve as the basis for the optimization of educational endeavours in cyberintelligence analysis. Therefore, we will analyse and discuss each of the high priority knowledge, skill and ability[5] from a teaching format perspective. Each high priority competence is discussed while taking into account particular topics of interest, examples and use cases, meaning that other researchers or educators could have different visions.

[5] Knowledge, skills and abilities discussed in this section can be found at the *NICE Framework: Current Versions* webpage on the *National Institute for Standards and Technology* website, available at https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-current-versions

• *K0315 - Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing information.*

One approach that could contribute to the successful knowledge transfer in this case is to structure the educational content by considering the stages of the intelligence cycle (CIA n.d.) and the cyberintelligence cycle - planning, collection, processing, analysis, dissemination and feedback (Recorded Future 2023). This is especially important given that the future cyberintelligence professionals will activate in intelligence and national security, but should also gain context dependent competences that, in this case, come from cybersecurity. Thus, methods, procedures and techniques should be taught by following each step of the intelligence and cyberintelligence cycle, with permanent links to the realm of cybersecurity (ex., technical equipment, sources of data in cybersecurity, levels of collection and analysis of threat intelligence).

• *S0229 - Skill in identifying cyber threats which may jeopardize organization and/or partner interests.*

In cyberintelligence professional settings, this skill is connected to the previous knowledge unit (i.e., K0315) as it is its foundation. In order to identify cybersecurity threats, one should understand how to ask oneself the right analytical questions and how to find the appropriate answers. Moreover, if the appropriate answers are found, it is important to integrate data that come from different sources and feeds of cyberintelligence. Many educational endeavours in cyberintelligence focus their efforts in the formation of this particular skill[6], but do not approach elements that are particular to the intelligence and national security field, such as collection from HUMINT. Integration of multiple sources and data specific to cybersecurity with HUMINT collection or other intelligence and national security-dependent types of sources is crucial in order to have a comprehensive understanding of a cybersecurity threat.

• *K0538 - Knowledge of target and threat organization structures, critical capabilities, and critical vulnerabilities.*

In order to make a proper transfer of this knowledge, the educator should focus the educational content around the understanding of the role and objectives of an organization. Besides these elements, understanding organization structures, critical capabilities and vulnerabilities is also dependent on understanding what the architecture of a particular IT&C infrastructure is and what particular elements are of critical importance. Thus, we believe that this knowledge can be trained by understanding management and risk analysis concepts and principles. This emphasizes the aforementioned idea that the cyberintelligence analyst should not

[6] *Mastering Cyber Threat Identification and Defense Strategies* by Public Sector Network, available at https://publicsectornetwork.com/event/online-training-mastering-cyber-threat-identification-in-the-public-sector/ and *Detecting and Mitigating Cyber Threats and Attacks* by Colorado University, available at https://www.coursera.org/learn/detecting-cyber-attacks

focus on possessing practical technical skills, but rather on understanding the technical elements that could support them in the analytical processes. In this particular case, if an organization is a victim of a cyber threat, the analyst should not only investigate the attacker, but also the victim. This way of thinking about the materialization of a cyber treat is implemented in the *Diamond Model* (Caltagirone 2020).

• *S0212 - Skill in disseminating items of highest intelligence value in a timely manner* and *S0210 - Skill in developing intelligence reports.*

We will approach both skills concurrently, because they refer to similar aspects, given the fact that intelligence dissemination depends on intelligence reporting. These skills are important not only for cyberintelligence analysis, but also for intelligence analysis in general. The US Government states on its Intelligence Careers website that "The final output of intelligence analysis is a carefully crafted intelligence report that provides political and military leaders with the information they need to make critical decisions. Skills central to the profession include analytical thinking and logical reasoning, the ability to write clear, concise reports and the ability to objectively analyse all sides of any given issue" (US Government n.d.). Still, cyberintelligence analysis is different from intelligence analysis performed in other national security branches, such as counterterrorism or counterespionage, given the fact that cyberintelligence analysis requires understanding and integration of technical aspects derived from cybersecurity investigations. This aspect generates the need for education and training endeavours specially designed to facilitate understanding and make it possible to operate with concepts specific to cyber threats, cyber vulnerabilities, tactics, techniques and procedures of hostile actors, our high priority competences being composed of such elements. Despite cybersecurity-derived knowledge units, the cyberintelligence analyst in intelligence and national security should be able to adapt to their beneficiary, given that not all decision-makers have the same level of understanding of cybersecurity technical aspects that could be a part of an intelligence product. If we corroborate this aspect with the reasonable expectation of not having a pattern for the actions performed by hostile threat actors, we infer that dissemination of high-quality intelligence products in a timely manner is crucial for countering any cyber threat. Thus, we believe that training actions for developing S0210 and S0212 are dependent on good practices and principles of intelligence analysis writing, one important work in this field being *Writing Classified and Unclassified Papers in the Intelligence Community* (Major 2009). Adding to this academic work, one could be able to identify training formats that focus on cybersecurity writing, such as *Cybersecurity Writing: Hack the Reader* (SANS Institute n.d.). Our educational approach regarding these particular skills and abilities would elaborate on Major's intelligence analysis writing principles while applying them to cybersecurity and cyberintelligence information.

• *K0110 – Knowledge of adversarial tactics, techniques, and procedures.*

While this is one of the most technical knowledge units from our set, from an educational perspective it is one of the most straightforward, if we consider the existence of *MITRE ATT&ACK Framework*[7], that is a database which consists of tactics, techniques and procedures specific to a large number of well-known threat actors. Also, given the fact that *MITRE ATT&CK Framework* contains definitions and use cases for every tactic, technique and procedure, it can be considered a really good educational resource, both for self-paced learning as well as for teacher-led formats. By gaining K0110, future cyberintelligence analysist in intelligence and national security, will be able to better understand how threat actors operate, how certain ways of operations interact and will be able to actively contribute to cyberintelligence investigations and to integrate technical data into cyberintelligence products designed to be disseminated to decision-makers.

• *S0359 – Skill to use critical thinking to analyse organisational patterns and relationships.*

Although critical thinking is a skill that can be educated with specific theoretical and practical content, we believe that in the context of cyberintelligence analysis training endeavours it might be one of the hardest to foster. As stated before, cyberintelligence analysis in intelligence and national security is highly dependent on contextual competences, which means that trainees and professionals in this field should be exposed to multiple use cases in real or fictious investigations, which can foster expert judgement ability and critical thinking skills. This perspective is complemented by Srinivas who states that the cyberintelligence analysts should imagine themselves in the role of a cyber attacker, in order to make the best possible analytical judgements (Srinivas 2018, p. 406). In order for this to happen, we insist on the fact that the cyberintelligence analyst should be exposed to many practical examples of cybersecurity and cyberintelligence investigations and case, that can diversify their expertise on this matter. Also, an important aspect for fostering critical thinking is to expose the cyberintelligence analyst to multiple and different analytical methods and ways of disseminating intelligence materials both theoretically and practically.

• *A0084 – Ability to evaluate, analyse, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/ intelligence products.*

Like S0359, we believe that A0084 is equally hard to train. This ability is rather trained on a continuum of educational activities, than by crafting and applying specific educational content and practical activities. Still, in a cyberintelligence analysis educational setting, one educator can propose to students' examples of fictitious use cases that are comprised of large quantities of data, both technical

[7] Available at URL: https://attack.mitre.org/

and non-technical, from which the students should extract the most important facts and perform assessments. For doing this kind of activities, cyberintelligence analyst should be able to apply structured analytical techniques, such as sorting, chronologies and timelines, event trees, event mapping and source check (US Defense Intelligence Agency 2008) and to possess good communication and organizational skills, especially when information is fragmented and contradictory and requires clarifications from collectors.

Conclusions

Starting from the research question – *How can we validate and prioritize knowledge, skills and abilities needed by the cyberintelligence analyst in intelligence and national security?* – we managed to achieve our research objective – *validate and prioritize the set of cybersecurity and intelligence competencies by applying a survey with the participation of cybersecurity, cyberintelligence and intelligence and national security experts*. In the first phase, we validated 86 out of the 95 cybersecurity and intelligence competences, most of them being clustered in analytical and context dependent competences. This shows us that cyberintelligence analysis is rather dependent on the type of organization where it is performed, intelligence and national security agencies, and on the specific context that is taken into account when performing an investigation, rather than on the technical aspects that are fundamental to the cybersecurity field. Thus, cyberintelligence analysis is more of an intelligence analysis subfield, rather than a cybersecurity one, proving that intelligence and national security organizations should consider crafting a profile of competences specific to their own organizational needs and subsequent training and education formats. In this context, relying separately on cybersecurity and intelligence courses and training endeavours is not sufficient and closing the gap in this matter consists in creating bespoke educational activities.

Also, we managed to classify as high priority eight out of the 86 priorly identified competences and to briefly elaborate on the specific educational practices and contexts that could be applied by educators in cyberintelligence analysis. In the particular context of these eight high priority competences, we believe that the educational approaches should combine cybersecurity and intelligence content, while understanding that cyberintelligence analysis competences can be trained over time, ideally by combing classical training formats with professional expertise. Thus, a cyberintelligence analyst learner profile should include intelligence analysis competences, dependent on knowledge, skills and abilities regarding collection, reporting, disseminating and sharing of information, and cybersecurity competences, dependent on knowledge referring to tactics, techniques and procedures of cyber hostile actors, cybersecurity vulnerabilities and critical capabilities. The utmost

important thing for a cyberintelligence analysis educator is to combine those elements and not teach them separately.

Regarding the limits of our research, we appreciate that the low response rate corroborated with the judgment sampling method, could induce bias to our results. Thus, in order to really test our research results it is important to verify them in real educational settings, by performing experimental studies, this being one of the future research directions.

A possible direction to continue our research would be to integrate the validated competences into a coherent cyberintelligence analysis professional framework, that could be used by employers and educators.

BIBLIOGRAPHY:

Alsmadi, Izzat. 2023. *The NICE Cyber Security Framework. Cyber Security Intelligence and Analytics Second Edition.* San Antonio, Texas: Springer.

Borum, Randy, and Ron Sanders. 2020. "Preparing America's Cyber Intelligence Workforce." *IEEE Security & Privacy* (IEEE) 18 (5): 67-73. Accessed August 24, 2023. doi:10.1109/MSEC.2020.3005035.

Borum, Randy, and Ron Sanders. 2020. "Preparing America's Cyber Intelligence Workforce." *IEEE Security & Privacy* 18 (5): 67 - 73. doi:10.1109/MSEC.2020.3005035.

Caltagirone, Sergio. 2020. *The Diamond Model of Intrusion Analysis.* ThreatIntellAcademy. https://www.threatintel.academy/wp-content/uploads/2020/07/diamond_summary.pdf

CIA. n.d. "Spy Kids." *Central Intelligence Agency.* Accessed December 7, 2023. https://www.cia.gov/spy-kids/parents-teachers/docs/Briefing-intelligence-cycle.pdf

Condruț, Cristian. 2023. "CYBERSECURITY KNOWLEDGE, SKILLS AND ABILITIES FOR INTELLIGENCE AND NATIONAL SECURITY ANALYSTS." *16th annual International Conference of Education, Research and Innovation.* Seville: IATED. 4200 - 4209.

Major, James. 2009. *Writing Classified and Unclassified Papers in the Intelligence Community.* New York: Scarecrow Press.

Nilsen, Richard. 2017. *Measuring Cybersecurity Competency: An Exploratory Investigation of the Cybersecurity Knolwledge, Skills and Abilities Necessary for Organizational Network Access Privileges.* Fort Lauderdale-Davie, Florida: Nova Southeastern University.

PennState. n.d. *Intelligence Writing.* Accessed December 7, 2023. https://www.e-education.psu.edu/geog571/node/431

Petersen, Rodney, Danielle Santos, Karen Wetzel, Matthew Smith, și Greg Witte. 2020. "The Workforce Framework for Cybersecurity (NICE Framework)." *NIST.* noiembrie. Accessed November 27, 2023. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

Recorded Future. 2023. *What the 6 Phases of the Threat Intelligence Lifecycle Mean for Your Team.* octombrie 24. Accessed December 7, 2023. https://www.recordedfuture.com/threat-intelligence-lifecycle-phases

SANS Institute. n.d. Accessed December 7, 2023. https://www.sans.org/cyber-security-courses/cyber-security-writing-hack-the-reader/

Sharma, Gaganpreet. 2017. "Pros and cons of different sampling techniques." *International Journal of Applied Research* 3 (7): 749 - 752.

Srinivas, Nowduri. 2018. "Critical Thinking and Best Practices for Cyber Security." *International Journal of Cyber-Security and Digital Forensics* (The Society of Digital Information and Wireless Communications) 7 (4): 391 - 409.

US Defense Intelligence Agency. 2008. *A Tradecraft Primer: Basic Structured Analytic Techniques.* Primer, Directorate for Analysis.

US Government. n.d. *CAREER FIELDS.* Accessed December 7, 2023. https://www.intelligencecareers.gov/career-fields#intelligence-analysis

Vitello, Sylvia, Jackie Greatorex, and Stuart Shaw. 2021. *What is competence? A shared interpretation of competence to support teaching, learning and assessment.* Cambridge: Cambridge University Press & Assessment.

STRATEGIC DIALOGUE

– Vice Admiral Mihai Panait, PhD, Chief of The Romanian Naval Forces –

Strategic Impact (S.I.): Vice Admiral Mihai Panait, welcome back to *Strategic Dialogue*.

In your previous interview you emphasized the issue of tensions in the region resulting from the Russian illegal annexation of Crimea. Meanwhile, these tensions have escalated, and the launch of the Russian invasion in February 2022 has brought the democratic world, which has expressed solidarity with Ukraine, face to face with Russia, as an aggressor. Moreover, in the Black Sea, both a bridge and a frontier between Europe and Asia, the Russian Federation has focused not only on preserving its sphere of influence and blocking the enlargement of the Western one, but also on pursuing the expansion of its own strategic interests.

Your perspective on the security situation in the Black Sea is of great value, both in your capacity as Chief of the Romania Naval Forces, and as an officer with extensive international expertise acquired in complex missions and high-level meetings with counterparts around the world as well.

S.I.: *In the light of the aforementioned considerations, we kindly ask you to share with our readers an informed viewpoint on the geopolitical reconfiguration of our neighbourhood.*

Vice Admiral Mihai Panait, PhD (VADM M.P.): The geopolitical reconfiguration of Romania's vicinity encompasses a range of significant factors, each of which exerts an influence on the country's security, economy and regional influence.

First, the Black Sea is a focal point of major powers' interests, including NATO, Russia, Türkiye and the European Union. Changes in naval power dynamics in this region have a direct impact on Romania.

Russia's invasion of Ukraine has increased the strategic importance of the Black Sea region for the security of NATO's eastern flank. The activity of the Russian Black Sea Fleet and the blocking of the maritime lines of communication pose a threat to the Alliance and its partner states (Moldova, Ukraine, Georgia). Although the Alliance's ability to operate in the Black Sea is limited by the Montreux Convention, NATO has helped to stabilize the area by increasing its military presence in the region and expanding cooperation with international partners.

Secondly, Romania is engaged in close collaboration with international partners with the objective of ensuring the security of the Black Sea. This includes participating in multinational exercises, exchanging information and coordinating security efforts, such as:

- SEA SHIELD – national exercise with international participation;
- EP MCM DIVE – national exercise with international participation (in cooperation with the 6th Fleet);
- ARIADNE – territorial waters of Greece;
- NUSRET – territorial waters of Türkiye;
- MCM POSEIDON – territorial waters of Bulgaria;
- Naval operation OSG – Mediterranean Sea;
- IRINI – Mediterranean Sea;
- SNMCMG-2 – Mediterranean Sea;
- TRITON – territorial waters of Bulgaria;
- BALTOPS – multinational joint exercise;
- MARE APERTO - maritime areas and coastal zones of the Tyrrhenian Sea, the Ionian Sea, the Adriatic Sea, and the Sardinian Sea.

I therefore believe that the geopolitical reconfiguration of Romania's neighbourhood is a complex and dynamic process, influenced by internal and external factors. Romania must continue to invest in modernizing its naval forces, strengthen its international alliances and adapt to new threats in order to ensure security and stability in the Black Sea region.

S.I.: *In this context, how has the balance of forces in the Black Sea region changed over the last two years, with specific reference to the role of naval forces?*

VADM M.P.: Over the last two years, the distribution of power in the Black Sea region has undergone significant changes, influenced mainly by increased tensions between Russia and the West, as well as by developments within NATO and countries bordering the Black Sea.

Since the beginning of the war, Russia's fleet has lost an impressive number of ships, significantly damaged or sunk by unmanned surface vehicle and missile attacks. Despite consequences, the Russian Black Sea Fleet maintains control over Crimea. In this context, the Russian fleet continues to enhance port security at its main naval bases and to improve port facilities in Kerci, Novorossisyk, Sochi and Tuapse in order to be able to continue its naval exercise. In addition, the presence of the Russian fleet in the Black Sea is likely to remain low because of the continued threat of Ukrainian missiles and USVs.

From the beginning, I would like to point out that the Russian Federation's unjustified military aggression against Ukraine has significantly changed the security landscape in the Black Sea region. The ongoing military confrontation, the large number of mines, unexploded ordnance (UXO) and other dangerous materials adrift in the Black Sea, and Russia's posture and continued aggressive intervention, by closing some areas and patrolling activity have had a significant impact on the level of maritime traffic. Black Sea riparian states are making great efforts to maintain the security of maritime transport routes.

Russia's invasion of Ukraine has created a variety of risks in the naval sector. The most problematic threat to merchant ships is hitting a marine mine. Since the beginning of the conflict Ukraine has launched 420 mines in accordance with Novorossiysk Navtex 2022. To date (27 of June, 2024) 103 mines have been confirmed and neutralized. Five mines have been found and destroyed in Romania's area of responsibility, including one near the entrance to the Port of Constanta under the Traffic Separation Scheme. This obviously creates problems regarding the safety of navigation and leads to high costs on the maritime industry such as fishing, offshore activities and tourism.

The distribution of power in the Black Sea region has changed significantly in the last two years, as Russia has strengthened its military presence, and NATO and its Allies have responded by reinforcing naval capabilities and intensifying multinational exercises. Along with other regional players, Romania has allocated resources towards the modernization of its fleet and naval infrastructure, in order to enhance its capacity to meet new security challenges.

Thus, the Romanian Naval Forces have facilitated the development of endowment and modernization plan that provides the most important programs:

• The "Coastal Defense and Anti-Ship Missile System", program which aims at equipping the Naval Forces with a system of four anti-ship missile launching systems;

• The "Minehunter" program representing the establishment of a mine warfare capability through the acquisition of two ships from the British Navy;

• The "Fast Intervention Diver Boat" program;

• The "ASuW- capability Helicopter" program;

• The "Assault Amphibious Vehicle – AA7" program which provides the Marine Infantry Regiment with 21 amphibious assault vehicles;

• Modernization program of 22-class frigates to upgrade combat capabilities and auxiliary systems;

• Missile Carrier Ships Modernization Program modernization of systems (energy, communications, navigation).

S.I.: *Despite Russia's long-standing dominance of the Black Sea from a naval perspective over the last decade, since 2022 its strategy has proven not so effective in the face of Ukrainian ingenuity in employing surface and underwater drones against Russian ships.*

Do you consider this to be a substantial change in the manner of conducting naval warfare, at least as far as the inland seas are concerned?

VADM M.P.: The use of unmanned surface vehicles (USVs) in this conflict poses a threat to maritime traffic, both for military and civilian ships. During the conflict, Ukraine has carried out more than 20 naval drone-attacks targeting military vessels in the Sevastopol and Novorossiysk naval bases and the Donuzlav and Kerch Straits.

I would like to emphasize that in 2024 the Russian Black Sea Fleet' activities were reduced due to the threat of unmanned surface vehicles operating at night. This was in response to the successful attacks by Ukraine, including on the patrol boat, Sergey Kotov. In late March, at least four Russian vessels were targeted by Ukraine.

As a result of its unique geography and facilities, which allow easy access from the sea to the Danube River, as well as its monitoring and warning capabilities on maritime threats, Romania plays a crucial role in securing maritime and inland waterway transport routes in the region.

In order to guarantee security of the river area, forces and means have been deployed, as follows:

• Surveillance and monitoring of river traffic in the area of responsibility of Romania and augmentation of the acknowledged maritime image;

• Providing pilotage service in the context of the massive traffic intensification on the maritime Danube;

• Use of autonomous unmanned systems;

• Protection of critical infrastructure and the Exclusive Economic Area through the development of maritime and river drone systems.

Another aspect that I would like to bring to your attention is that, as a result of the fact that the Russian Federation did not agree to the extension of the Black Sea Grain Initiative to 2023, Ukraine has started to use its ports on the Danube River. To

prevent this, Russian Armed Forces have attacked Ukrainian infrastructure on the Danube using drones. These types of drones have been used throughout the conflict in attacks against other regions of Ukraine. Attacks on Ukrainian infrastructure (Reni, Ismail) are also have an impact in Romania.

Concurrently, other risks are associated with the use of the Danube River for grain transit:

- Increased risk of collision;
- Increased risk of maritime pollution;
- Increased threat of collision with maritime mines.

***S.I.*:** *It is acknowledged that the Romanian Naval Forces play an important role in maintaining regional and international stability.*

Has the war in Ukraine resulted in far-reaching changes in the direction of mission development of this category of forces?

VADM M.P.: Romania's national interest is to maintain freedom of navigation on the Black Sea and the Danube River; to this end, Romanian Naval Forces promote and defend national interests and sovereign rights at sea and on the river, independently, in a joint force or as part of a multinational force. Furthermore, the Naval Forces continue to be an active contributor to regional security and stability, as part of various cooperation initiatives in the Wider Black Sea Area.

The Romanian Naval Forces must be able to fulfil the following missions:

- contribute to national security;
- defend national sovereignty and integrity;
- contribute to collective defence;
- promote regional and global stability;
- support local authority in civil emergency management.

The Romanian Naval Forces maintain the freedom of navigation of maritime communication lines, which are a critical factor for economic development and prosperity.

The Naval Forces have adopted their own tactics, techniques and procedures by planning and conducting mine surveillance and systematic actions of active search. The forces used in these actions consisted of warships, helicopters, drones and EOD teams. Additionally, support was provided by other military structures, the Coast Guard and maritime patrol aircraft (from France, the USA, and Türkiye).

The Romanian Naval Forces have engaged in numerous procurement programs that will ensure the availability of the capabilities required to meet the challenges of the current security environment in the Black Sea. Our organisation is engaged in a number of projects, of which a NATO-level project – Maritime Unmanned System (MUS), one as part of the EU initiative - Permanent Structured Cooperation

(PESCO) – Maritime (semi-) Autonomous Systems for Mine Countermeasures (MAS MCM), PESCO EUNDC – with the main objective to develop a network of diving centres in the EU Member States and one in MDA-ASW.

The MUS initiative allows participating nations to work together to integrate all existing data into the supply of military equipment manufacturers or the data extracted from their own experience to create a common picture of the present and future of maritime unmanned systems. Areas of cooperation are: information exchange, standardization, doctrine development, operational research and experimentation, logistics, training, procurement and military industry partnerships.

The objective of the PESCO MAS MCM project is to provide, in the medium and long-term, a diverse world-class of underwater, surface and airborne (semi-) autonomous maritime mine action technologies in order to increase cooperation between Member States, reduce Member States' efforts in this field, enhance interoperability, address gaps and reinforce the industrial and technological base. The project aims to support future common procurement to reduce research costs, create prototypes and mass production.

European Union Network of Diving Centres (EUNDC) is a PESCO project with the main objective of creating a network of diving centres to facilitate the coordination of diver certification and training at EU-level, based on common standards and procedures, as well as their certification for European missions. Interoperability between diving centres can facilitate the coordination of common operations, strengthening EU's capacity to respond to common threats to maritime security and other environmental and security challenges.

Also, within the MDA-ASW project carried out in collaboration with the strategic partner, the Romanian Naval Forces are engaged in dialogue to be equipped with maritime unmanned systems to improve electro-acoustic surveillance at the Black Sea. The development of autonomous vehicles, using cutting-edge technology and an operational architecture, with a modular configuration, will significantly contribute to EU maritime security, helping to counter the threat of sea mines.

S.I.: *At operational level, an important element of the war in the proximity of Romania is the threat of sea mines. In the first part of this year, the Romanian Armed Forces was approved to take part in operations under the aegis of the Task Force to Counter the Sea Mines in the Black Sea (MCM Black Sea), alongside Bulgarian and Turkish naval forces. We kindly request further elaboration on this component of the Naval Forces' missions.*

What are the most important lessons identified so far from mine warfare?

VADM M.P.: The war in Ukraine is a reminder that while modern technology can bring advantages over older systems, quantity still matters. The conflict once

again proved the pivotal role of technological and industrial companies' capabilities in warfare. Also, the use of cheap unmanned systems has increased significantly with favourable outcomes.

The recent signing of the "Trilateral Initiative" between Bulgaria, Türkiye, and Romania for the establishment of a Task Force to Counter the Sea Mines in the Black Sea (MCM Black Sea) is a proof of the political will of the countries in the region to get involved in ensuring maritime security against the threat of drifting mines in the Black Sea.

This initiative, which has its origins in close collaboration and mutual understanding between the three allied nations, represents a crucial step in addressing the threat of sea mines and ensuring safe navigation.

The Memorandum of Understanding outlines a clear and efficient operational structure. With a rotating command every six months and a minimum of two planned activations in each rotation, a reliable framework has been established to ensure vigilance and continuous readiness.

The first activation of the task group was on July 2nd, for a 15-day period, during which the Romanian Naval Forces engaged with a minesweeper vessel. This structure not only increases the collective operational capabilities, but also addresses the conflict in our region, which required the mobilization of the three NATO Black Sea-bordering countries to ensure freedom of navigation, in compliance with the Montreux Convention.

The primary objectives of the MCM BS Task Group are:

- conducting reconnaissance and surveillance operations against the threat of naval mines in the Black Sea;

- conducting MCM operations in designated areas and related SAR operations, if required;

- integrating forces and participating in common exercises to share expertise and improve interoperability;

- identifying ways and means of collaborating and ensuring complementarity, with SNMCMG-2 and other relevant allied non-coastal operations when present in the Black Sea, in accordance with the Montreux Convention. Where appropriate, such collaboration could include unmanned systems, intelligence, maritime patrol aviation, special operation and boarding teams, EOD;

- contributing to raising awareness of NATO's maritime situation in the Black Sea;

- conducting visits to the ports of the participants for cultural exchange and improving mutual understanding;

- performing other tasks within the scope of this Memorandum of Understanding as agreed by the three parties.

S.I.: *The Washington Summit in July 2024 has marked NATO's 75th Anniversary. In its final Declaration, NATO reaffirmed its continued support for regional efforts undertaken by Allies with the objective of upholding security, safety, stability and freedom of navigation in the Black Sea region (in compliance with the Montreux Convention).*

Please provide your opinion on how Alliance's contribution in the area can be increased, and what would this entail in the field of maritime security?

VADM M.P.: In the light of the ongoing discussions in the aftermath of the NATO Summit in Washington, it is imperative to reiterate the strategic importance of the Black Sea and to reinforce the measures taken to ensure regional security.

To increase NATO's contribution in the Black Sea, I consider that certain measures are needed to bolster military presence, strengthen the national capabilities of the littoral states and promote regional cooperation.

To deter aggressive actions and to demonstrate our commitment to regional security, the organisation of regular patrols and common exercises between the naval forces of NATO member states in the Black Sea is essential. The rotational and permanent deployment of an increased number of NATO vessels in the Black Sea will ensure a continuous presence and the ability to rapidly respond to any incidents, thus enhancing maritime security.

Providing technical and logistical support to Romania and Bulgaria, to modernize fleets and maritime infrastructure will enhance national capabilities and facilitate regional cooperation. The implementation of training programs and effective information exchange mechanism for their maritime forces will improve readiness and coordination.

Advancing cooperative initiatives among riparian states to develop common maritime security strategies will reinforce regional solidarity and responsiveness to threats. MARSEC COE is a regional centre of excellence for maritime security acting as a hub for maritime security research, training and cooperation in the area of maritime security, strengthening regional capabilities and facilitating the exchange of best practices.

Investments in modernizing ports and logistics support infrastructure are essential to facilitate an effective naval presence and improve logistical capabilities. The deployment of advanced surveillance technologies and early warning systems will enable effective monitoring of maritime activities and prompt response to any threat, thus ensuring the continued protection of the region.

The implementation of these measures will enable NATO to significantly enhance maritime security in the Black Sea. Strengthened military presence and national capabilities will serve to deter threats, while regional cooperation will enable a coordinated and effective response to security challenges. Investments in

technology and infrastructure investments will ensure continuous monitoring and protection of the region. These actions will not only strengthen maritime security, but they will also demonstrate NATO's firm commitment to the stability and protection of its Allies and Partners in this strategic region. Essentially, through a comprehensive and coordinated approach, NATO can ensure a robust and effective presence in the Black Sea, thus contributing to long-term peace and security in this vital area.

As far as Romania is concerned, the maritime security strategy must be the programmatic document adapted to respond effectively to the challenges posed by the Russian-Ukrainian conflict. Such a strategy should be aligned with the strategic objectives of the European Union and NATO in the Black Sea region and emphasize Romania's national interests in the Black Sea and the Danube. The strategy will set the policy development of all ministries that will address maritime security.

Key elements of Romania's maritime security strategy will be based primarily on international cooperation by strengthening partnerships with NATO and EU to ensure a robust military presence in the Black Sea and on active participation in security exercises and operations, as well as the intelligence sharing with Allies.

Secondly, this strategy will facilitate the acquisition of new naval capabilities and the modernization of outdated ones by investing in fleet and equipment modernization as well as developing cyber warfare and intelligence capabilities to counter Russian hybrid threats.

Security of critical infrastructure, port protection, offshore extraction platforms, gas pipelines, and cables against attacks will be an important chapter of the strategy, along with the implementation of rigorous security measures for maritime transportation and Danube infrastructure for grain and general cargo.

If we consider the threat posed by drifting mines, the freedom of navigation, the environmental and resource protection, the promotion of Romania's economic interests by ensuring safe trade routes, we think of another chapter of Romania's maritime security strategy.

Implementing such a strategy, Romania will not only ensure its maritime security in a complex regional context, but will also contribute to collective stability and security in the Black Sea, in line with EU and NATO strategic objectives.

***S.I.*:** *In your work published this year by the "Mircea cel Bătrân" Naval Academy Publishing House, entitled "Leadership and Security in the Black Sea", you assert that "The Romanian Naval Forces serve as a pivotal element in the reinforcement of regional security, a promoter of security culture, a genuine instrument for the implementation of state diplomacy at sea, leadership through cooperation being a way to guarantee credibility by assuming commitments which, at the level of the Romanian Naval Forces, are translated into a wide range of national and multinational missions".*

In the light of the concept of "leadership through cooperation", what is your assessment of the role that Romania should play in the future Black Sea security architecture? How would you evaluate Romania's contribution within the Three Seas Initiative?

VADM M.P.: In the context of the Black Sea security architecture, Romania has a major responsibility in ensuring security and stability in this strategic region. The Black Sea is not only a transit area for energy and maritime routes, but also a vital geographical border for Europe's energy and geopolitical security. The Romanian Naval Forces must be prepared to respond rapidly to security challenges, including by participating in multinational exercises and operations in close cooperation with NATO and regional Allies.

As part of the Three Seas Initiative, Romania can play a leading role in promoting regional security cooperation. The initiative brings together Central and Eastern European states in a framework of strategic collaboration, focused on infrastructure, energy and security. The Romanian Naval Forces can support this initiative by facilitating dialogue and organizing common exercise with partner states to strengthen operational capabilities and interoperability in the maritime domain.

The Romanian Naval Forces actively participate in conferences with other NATO member states in order to facilitate dialogue: The Black Sea Maritime Forum, organized in 2022 and 2024 in Bucharest, SEA BREEZE 23-2 Maritime Commanders Planning Conference, organized in 2023 in Constanta.

In conclusion, Romania's role in the future security architecture of the Black Sea and the Three Seas Initiative must be that of a leader and promoter of regional stability. By assuming an active leadership in naval and military cooperation, Romania can strengthen its credibility and influence in the region, thus contributing to the common security and prosperity of the partner states in Central and Eastern Europe.

S.I.: *Finally, we would be particularly interested to receive your perspective on how you assess the situation in the Black Sea in the context of the elaboration of future strategic documents, namely Romania's National Defence Strategy, the White Paper, and the Military Strategy. We would also be interested to receive your assessment of the priorities that Romania should adopt in terms of naval forces in the coming period.*

VADM M.P.: With regard to issuing the National Defence Strategy, the White Charter and the Military Strategy, Romania's priorities in terms of naval forces should reflect the strategic importance of the Black Sea and the need to respond effectively to the security challenges in this region. In my opinion, the priorities

should include strengthening operational capabilities, modernizing the fleet, and increasing international cooperation

In the first instance, it is essential to strengthen the operational capabilities of the Romanian Naval Forces. This will entail an increase in the level of personnel training, the conduct of joint and multinational exercises and improvement in interoperability with our NATO Allies. The development of rapid and flexible response capabilities is crucial to deal with asymmetric threats and to ensure the protection of maritime critical infrastructure.

Secondly, modernization of the naval fleet is a top priority. This involves acquiring modern vessels equipped with advanced technology, capable of operating effectively in a complex and dynamic environment. In particular, we should invest in multirole frigates and corvettes, patrol vessels and surveillance and reconnaissance equipment. The modernization of the fleet will enhance our ability to ensure maritime security and contribute to NATO and EU missions.

Another priority is increasing international cooperation, both within NATO and with regional partners. Working closely with our Allies, sharing intelligence and participating in common exercises are essential to ensure a coordinated and effective approach to threats. We should also promote bilateral and multilateral partnerships with Black Sea littoral states to develop a common maritime security strategy.

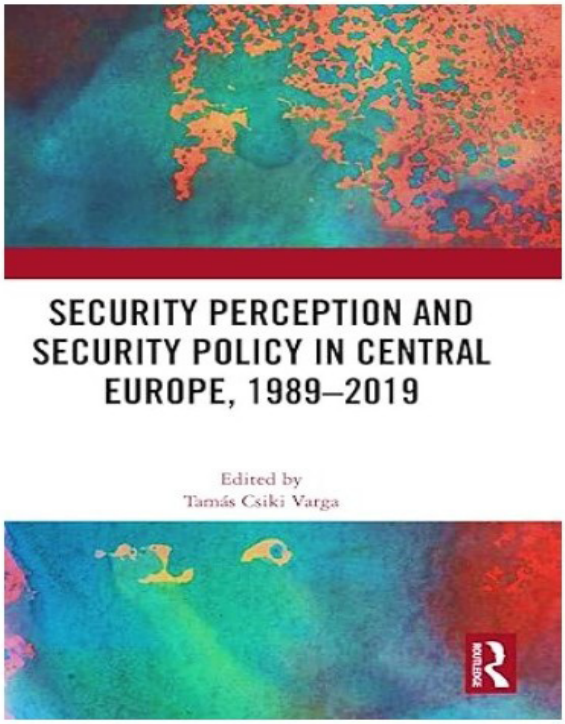
In conclusion, Romania's priorities in terms of naval forces, in the context of future strategic documents, should focus on strengthening operational capabilities, modernization of the fleet and increased international cooperation. These measures will ensure an effective defence of national interests and contribute to stability and security in the Black Sea region, reflecting our strong commitment to the North Atlantic Alliance and to our regional partners.

S.I.: *Vice Admiral Mihai Panait, thank you very much for sharing with the readers of Strategic Impact your most valuable insights on the Black Sea issues and the role of the Romanian Naval Forces in the new security context.*

CENTRAL EUROPE, SIMILARITIES AND DIFFERENCES IN SECURITY POLICY

- edited by Tamás Csiki Varga -

Mihai Zodian**, **PhD*



Security Perception and Security Policy in Central Europe, 1989-2019, Routledge, 2024, 160 pages.

The volume contains an introduction by Tamás Csiki Varga and nine chapters by: Ádám Budai, Tomáš Čižik, Zdeněk Kříž, Hennadiy Maksak, Tamás Levente Molnár, Milena Palczewska, Alexandra Sarcinschi, and Aleksandar Vanchoski. The states covered are Hungary, Slovakia, Czechia, Ukraine, Austria, Poland, Romania, Croatia, and Serbia.

***Keywords**: Central Europe; Ukraine; security; security policy; structured and focused comparison; NATO; EU; military power; Russia.*

Central Europe has made a bit of a comeback in public attention after Russia's renewed aggression against Ukraine in 2022. *Security Perception and Security Policy* offers an empirical approach to the region's politico-military issues, and it is written by local experts, using a very pragmatic and concise style. The book is the result of an international research, involving several institutes in the region[1].

**** Mihai Zodian, PhD, is a Researcher at the Centre for Defence and Security Strategic Studies within the "Carol I" National Defence University, Bucharest, Romania. E-mail: zodian@gmail.com***

[1] To warn against a possible conflict of interests, one of the authors is a personal colleague and I participated in a different section of the same research project.

The term Central Europe is often politicized, but the editors opted for an inclusive approach, which increases the utility of this product.

I recommend *Security Perception and Security Policy* to anyone interested in the events of this space and on their background. The chapters contain a high degree of contextualization, a description of the official policies, and of the main turns and twists during the 30 years it covers. It helps the reader to understand current decisions and attitudes, especially the differences between Central European states. The volume is also interesting because of the methodological practices of its authors.

Security Perception and Security Policy follows the structured-focused comparison practice of investigation. This approach takes the classical method of looking for similarities and differences between some objects and adds more direction and precision to it (George and Bennett 2005). It was promoted as a qualitative alternative to statistical-inspired scientific investigation with the promise of more depth and nuance, while keeping the main tenets of positivism. This approach has grown in stature in the last decades and is close to the reformed research practices of the case study by process tracing (George and Bennett 2005).

Thus, the chapters share a common framework of themes to investigate. The main research directions are security perceptions, foreign policy orientation, level of ambition and policy issues. Most states were influenced by the fall of Communism, the transition to democracy and market economy, and the orientation of foreign policy away from Moscow and toward the West. Here, NATO and EU integration represented the main goal of regional political elites. Often forgotten in current debates regarding the responsibility for Russia's aggression against Ukraine is the fact that countries in Central Europe played an active role in pressing for the enlargement of both transatlantic organizations.

For example, Poland led the wave of changes in the late 1980s and then, emphasized independence and Euro-Atlantic integration. Threat perception was oriented, in the 2010s, towards internal phenomena like poverty and aging, but there was a growing emphasis on the risk of war in the region. The most important security policy goal was to avoid Russian domination, a goal shared by most states (Palczewska 2024, 85). For this reason, the partnership with the United States represents a salient pillar of Polish security policies, but European defence may also be taken into consideration.

By contrast, Hungarian society considered that military threats were less important after the fall of Communism and of the Soviet Union. Domestic issues were salient, especially the ones related to welfare, prices, and public safety. Hungary was one of the first NATO and EU members from Central Europe, and its security policy was linked to the integration process or the decisions of these two organizations. It also emphasized neighborhood strategies and actions, migration policies, and a degree of pacifism in international affairs (Budai 2024).

Romania joined NATO and EU later as it was interested in domestic security reform and was concerned about Russia's intentions and policies. The internal policies and collective memory had a major impact on security perceptions, which also stressed welfare issues or prices, and were less preoccupied with international terrorism or migration in comparison with other European societies (Sarcinschi 2024, 99). Like in Poland, the importance of war as a security threat grew after Russia's conflict of 2008 with Georgia and its aggression against Ukraine which began in 2014 and expanded in 2022. Romania's foreign policy was oriented towards NATO, the EU, and the United States.

Ukraine tried to steer a middle course. It attempted to remain a neutral state, with an independent democracy and a defensive military policy, until Russia's interferences and the invasion of 2014 pushed the state towards the West (Maksak 2024). NATO membership was promised in vague terms at the Bucharest Summit in 2008, but a combination of internal and external factors kept Ukraine away from the alliance. The Revolution of Dignity (the Maiden Protests) and Putin's aggression made Russia the main threat, and the West the main source of support (Maksak 2024, 57-59).

There are a total of nine case studies. *Security Perception and Security Policy* shows the commonalities and the differences between the Central European states with brief and easy-to-read chapters, containing a lot of data on public opinion and security documents. The main drawbacks of this volume are the emphasis on formal texts, which may confuse a reader unaccustomed to the context, and the lack of a separate chapter for conclusions and comparisons.

That being written, it is my belief the book is valuable for any reader interested in the region, due to its thematic and coherent nature, that structured and focused comparison should become the rule for most collective and comparative research project in Romania and I hope that the volume will inspire further research, for example, concerning the decision making processes and their sources.

BIBLIOGRAPHY:

Budai, Ádám. 2024. "The security perception and security policy of Hungary, 1989–2018." In *Security Perception and Security Policy in Central Europe, 1989-2019*, by Tamás Csiki (ed.) Varga. New York: Routledge .

George, Alexander L., and Andrew Bennett. 2005. *Case studies and theory development in the social sciences*. Cambridge: MIT Press.

Maksak, Hennadiy. 2024. "The security perception and security policy of Ukraine, 1991-2018." In *Security Perception and Security Policy in Central Europe, 1918-2019*, by Tamás Csiki (ed.) Varga. New York : Routledge.

Palczewska, Milena. 2024. "The security perception and security policy of Poland, 1989–2017." In *Security Perception and Security Policy in Central Europe, 1989-2019*, by Tamás Csiki (ed.) Varga. New York : Routledge .

Sarcinschi, Alexandra. 2024. "Security perception and security policy in Romania since the 1989 Revolution." In *Security Perception and Security Policy in Central Europe, 1989-2019*, by Tamás Csiki (ed.) Varga . New York: Routledge.

INTERNATIONAL SEMINAR

"Lessons identified from the conflict in Ukraine"

16th May, 2024

The Centre for Defence and Security Strategic Studies (CDSSS) within "Carol I" National Defence University (NDU) was the host of the second edition of the International Seminar on *"Lessons identified from the conflict in Ukraine"*, which took place on 16th May 2024.

This year's edition of the Seminar was held in hybrid format, online on the E-Learning platform ILIAS DIDAD and on-site, in the University Senate Hall, according to the CDSSS Agenda with the main activities for the academic year 2023-2024, document approved by the Commandant of "Carol I" NDU.

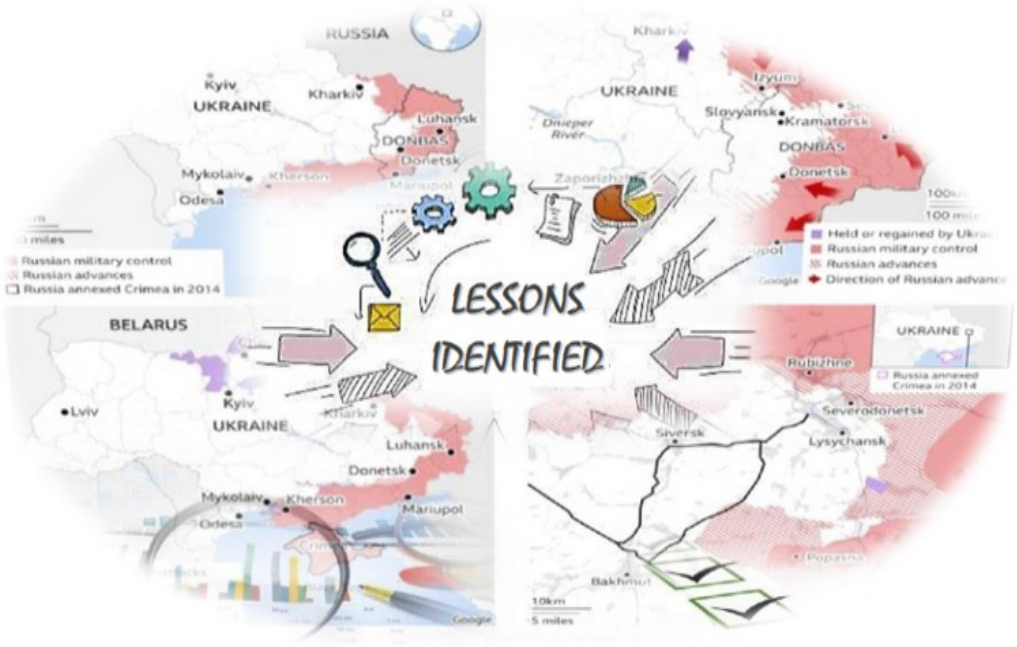


Photo: *Aspect of the International Seminar*

The event aimed to analyse certain aspects regarding the evolution of the conflict in Ukraine and the lessons identified in the conduct of the armed conflict. The main objectives referred to the analysis of the implications of the events taking place in Ukraine – targeting the following dimensions: political, military, legal, economic, social, informational, and humanitarian. Also, the event aimed at the identifying the main threats at national and international level, as well as, analysing the major consequences in terms of regional and global stability and security generated by the scale of the armed conflict.

More than two years after the invasion of Ukraine by the Russian Federation, at dawn on February 24th, 2022, the largest attack on a European country since the Second World War, the security situation in the South-East European region remains extremely tense and continues to pose a real threat to European security, but also to the Alliance. We find ourselves in a particularly complex international context with multiple challenges on the political, military, legal, economic, social, informational and humanitarian dimensions. The sacrifice and suffering of the Ukrainian people in the face of Russian aggression appeals to the international community to morally and politically continue and step up its support for Ukraine.

In the opening speech of the Seminar, the Commandant (Rector) of "Carol I" NDU, Major General Eugen MAVRIȘ, presented several aspects of the current security environment, more than two years after the outbreak of the war in South-Eastern Europe, caused by the unprovoked invasion of the Russian Armed Forces on Ukraine, a

Photo: *Aspect of the International Seminar*

situation that had a profound impact on the international security environment, generating a large-scale military conflict in the Romanian vicinity. At the same time, the Commandant (Rector) conveyed to those present: "I strongly believe that the scientific event will constitute an opportunity for all of us to gain a better grasp of the solutions for today's challenges and to develop new ideas regarding the effects on national, regional and international security. Their development may contribute to achieving success in training and conducting future warfare."

Photo: *Aspect of the International Seminar*

The activity was moderated by Colonel PhD Florian CÎRCIUMARU, CDSSS Director, and Colonel PhD Dan-Lucian PETRESCU, Head of the Strategic Analysis and Evaluations Office within CDSSS. The Organizing Committee of the Seminar, under the coordination of the CDSSS Director, included the management staff of the Centre, as well as the members of the specialized microstructure –Scientific Secretariat, Events and Collaborations Department.

The seminar brought together numerous specialists, both military and civilian, members of the national and international scientific community, representatives of military and civilian higher education institutions of Ukraine (National Defense University of Ukraine; "Taras Shevchenko" National University in Kyiv; Institute of Military Law, Kharkiv; "Igor Sikorsky" Kyiv Polytechnic Institute), the representative of NATO Liaison Office in Kyiv, representatives of the operational institutions and structures within the Ministry of National Defence (Combined Forces

Command, Air Staff, Naval Staff, Training and Doctrine Directorate, Department for Defence Policy, Planning and International Relations, Regional Department of Defense Resources Management Studies), the Association of Reserve Officers from Romania, representatives of the National System of Defense, Public Order and National Security and, also, CDSSS research staff.

Photo: *Aspect of the International Seminar*

Based on the theme of the event, the debates focused on four topics: the rhetoric of nuclear proliferation, the role of CIMIC in conflict, hybrid warfare techniques (disinformation, propaganda, manipulation), issues of violations of International Humanitarian Law, other rights, and the consequences of the war.

Therefore, the proposed theme provided the framework for 22 presentations, in English, which were debated:

- *"THE IMPORTANCE OF LL SYSTEM IN EDUCATION AND TRAINING SYSTEM"*
- *"RUSSIAN WAR AGAINST UKRAINE LESSONS LEARNED CURRICULUM GUIDE: MAY 2024 PERSPECTIVES "*
- *"INFORMATION CHALLENGES OF LARGE-SCALE RUSSIAN AGRESSION AGAINST UKRAINE"*
- *"RUSSIAN-UKRAINIAN WAR: THE CHALLENGES OF CIVIL-MILITARY RELATIONS"*
- *"RUSSIAN INVASION: EXPECTATIONS VS REALITY"*
- *"NUCLEAR RHETORIC IN RUSSIA'S WAR AGAINST UKRAINE"*

- *"THE NUCLEAR DIMENSION: WAR, COERCIVE DIPLOMACY AND THE LIMITS OF INTERNATIONAL SECURITY"*
- *"ADDITIVE MANUFACTURING AND PROLIFERATION CONTROL OF THE UNMANNED AERIAL SYSTEMS IN THE CONTEXT OF THE UKRAINE CONFLICT"*
- *"MAINTENANCE ASPECTS OF UKRAINIAN DRONES"*
- *"THE POSSIBLE EFFECTS OF HYBRID WARFARE ON THE SECURITY OF THE MEMBER STATES OF THE EUROPEAN UNION IN THE CONTEXT OF THE UPCOMING EUROPEAN PARLIAMENT ELECTIONS"*
- *"GOVERNANCE CONTINUITY AND BUSINESS RESILIENCE – LESSONS IDENTIFIED FROM UKRAINE"*
- *"INTEGRATED EDUCATIONAL INFRASTRUCTURES FOR INTELLIGENT LEARNING: DIGITAL WARFARE"*
- *"ROLE OF GENERAL INSPECTORATE FOR EMERGENCY SITUATIONS IN MANAGING THE INFLUX OF PEOPLE FROM THE RUSSIAN-UKRAINIAN CONFLICT ZONE"*
- *"CHALLENGES FOR FREEDOM OF NAVIGATION IN BLACK SEA REGION"*
- *"NEW LESSONS IDENTIFIED DURING THE SECOND YEAR OF WAR IN UKRAINE"*
- *"WHERE ARE WE HEADING? WHAT WILL BE THE NEW POLITICAL, ECONOMIC, AND MILITARY ORGANIZATION IN THE FUTURE?"*
- *"DEFICIENCIES OF THE MILITARY TRAINING SYSTEMS OF THE ARMED FORCES INVOLVED IN THE WAR"*
- *"THE RUSSIAN-UKRAINIAN WAR. ACTS OF VIOLATION OF INTERNATIONAL HUMANITARIAN LAW AND THEIR PUNISHMENT"*
- *"THE CHALLENGE OF BALANCING SOCIAL COHESION AND THE HUMANITARIAN CRISIS IN UKRAINE"*
- *"LESSONS IDENTIFIED ON DISINFORMATION IN THE CONTEXT OF OVER TWO YEARS OF WAR IN UKRAINE"*
- *"THE ECONOMIC EFFECTS OF THE WAR IN UKRAINE"*
- *"ROOT CAUSE ANALYSIS THE HUMAN LOSSES IN THE CONFLICT IN UKRAINE. LESSONS IDENTIFIED IN THE CONDUCT OF THE CONFLICT".*

At the end of the activity, the conclusions were presented on the results of the scientific endeavor, which achieved its goal this time as well, the scientific character of the event being fully realized, demonstrating once again the major common concern on security at national and regional level.

Information about upcoming events organized by CDSSS can be found on the website: https://cssas.unap.ro/ro/manifestari.htm

Otilia LEHACI , PhD*

Otilia LEHACI, PhD, works within the Scientific Events Department of the Centre for Defence and Security Strategic Studies within "Carol I" National Defence University, Bucharest, Romania. E-mail: otilia.lehaci@unap.ro

GUIDE FOR AUTHORS

We welcome those interested in publishing articles in the academic journal *Strategic Impact*, while subjecting their attention towards aspects to consider upon drafting their articles. **Starting with issue no. 1/2023, the journal shall be published in the English language only!**

MAIN SELECTION CRITERIA are the following:

- ✓ **Compliance with the thematic area of the journal – security and strategic studies** and the following topics: political-military topical aspects, trends and perspectives in security, defence, geopolitics and geostrategies, international relations, intelligence, information society, peace and war, conflict management, military strategy, cyber-security;
- ✓ **Originality** of the paper – own argumentation; novelty character – not priorly published;
- ✓ **Quality of the scientific content** – neutral, objective style, argumentation of statements and mentioning of all references used;
- ✓ **A relevant bibliography**, comprising recent and prestigious specialized works, including books, presented according to herein model;
- ✓ **English** language shall meet academic standards (British or American usage is accepted, but not a mixture of these).
- ✓ **Adequacy to the editorial standards adopted by the journal.**

EDITING NORMS

- ✓ **Article length** may vary between **6 and 12 pages** (25.000 - 50.000 characters), including bibliography, tables and figures, if any.
- ✓ **Page settings**: margins – 2 cm, A 4 format.
- ✓ The article shall be written in **Times New Roman font, size 12, one-line spacing.**
- ✓ The document shall be saved as Word (.doc/.docx). The name of the document shall contain the author's name.

ARTICLE STRUCTURE

- ✓ **Title** (centred, capital, bold characters, font 24).
- ✓ **A short presentation of the author**, comprising the following elements: given name, last name (the latter shall be written in capital letters, to avoid

confusion), main institutional affiliation and position held, military rank, academic title, scientific title (PhD title or PhD Candidate – domain and university), city and country of residence, e-mail address.

- ✓ A relevant **abstract**, not to exceed 150 words (italic characters)
- ✓ 6-8 relevant **keywords** (italic characters)
- ✓ **Introduction / preliminary considerations**
- ✓ **2 - 4 chapters** (numbered, starting with 1) (subchapters if applicable)
- ✓ **Conclusions**.
- ✓ **Tables / graphics / figures**, if they are useful for the argumentation, with reference made in the text. They shall be also sent in .jpeg /.png/.tiff format as well.

In the case of tables, please mention above "**Table no. X**: Title", while in the case of figures there shall be mentioned below (e.g. maps, etc.), "**Figure no. X:** Title" and the source, if applicable, shall be mentioned in a footnote.

REFERENCES

It is academic common knowledge that in the Abstract and Conclusions there shall not be inserted any references.

The article shall have references and bibliography, in the form seen below. Titles of works shall be mentioned in the language in which they were consulted, with transliteration in Latin alphabet if there is the case (e.g. in the case of Cyrillic, Arabic characters, etc.). Please provide English translation for all sources in other languages.

The article will comprise in-text citation and bibliography (in alphabetical order), according to The Chicago Manual of Style[1], as in examples below:

BOOK

Reference list entries (in alphabetical order)

Grazer, Brian, and Charles Fishman. 2015. A Curious Mind: The Secret to a Bigger Life. New York: Simon & Schuster.

Smith, Zadie. 2016. Swing Time. New York: Penguin Press.

In-text citation

(Grazer and Fishman 2015, 12)

(Smith 2016, 315–16)

[1] URL: https://www.chicagomanualofstyle.org/tools_citationguide/citation-guide-2.html

CHAPTER OF AN EDITED BOOK

In the reference list, include the page range for the chapter. In the text, cite specific pages.

Reference list entry

Thoreau, Henry David. 2016. "Walking." *In The Making of the American Essay*, edited by John D'Agata, 167–95. Minneapolis: Graywolf Press.

In-text citation

(Thoreau 2016, 177–78)

ARTICLE

In the reference list, include page range for the whole article. In the text, cite specific page numbers. For article consulted online, include a URL or the name of the database in the reference list entry. Many journal articles list a DOI (Digital Object Identifier). A DOI forms a permanent URL that begins https://doi.org/. This URL is preferable to the URL that appears in your browser's address bar.

Reference list entries (in alphabetical order)

Keng, Shao-Hsun, Chun-Hung Lin, and Peter F. Orazem. 2017. "Expanding College Access in Taiwan, 1978–2014: Effects on Graduate Quality and Income Inequality." *Journal of Human Capital* 11, no. 1 (Spring): 1–34. https://doi.org/10.1086/690235.

LaSalle, Peter. 2017. "Conundrum: A Story about Reading." *New England Review* 38 (1): 95–109. Project MUSE.

In-text citation

(Keng, Lin, and Orazem 2017, 9–10)

(LaSalle 2017, 95)

WEBSITE CONTENT

Reference list entries (in alphabetical order)

Bouman, Katie. 2016. "How to Take a Picture of a Black Hole." Filmed November 2016 at TEDxBeaconStreet, Brookline, MA. Video, 12:51. https://www.ted.com/talks/katie_bouman_what_does_a_black_hole_look_like

Google. 2017. "Privacy Policy." Privacy & Terms. Last modified April 17, 2017. https://www.google.com/policies/privacy/

Yale University. n.d. "About Yale: Yale Facts." Accessed May 1, 2017. https://www.yale.edu/about-yale/yale-facts

Citare în text

(Bouman 2016)

(Google 2017)

(Yale University, n.d.)

NEWS OR MAGAZINE ARTICLES

Articles from newspapers or news sites, magazines, blogs, and like are cited similarly. In the reference list, it can be helpful to repeat the year with sources that are cited also by month and day. If you consulted the article online, include a URL or the name of the databases.

Reference list entries (in alphabetical order)

Manjoo, Farhad. 2017. "Snap Makes a Bet on the Cultural Supremacy of the Camera." *New York Times*, March 8, 2017. https://www.nytimes.com/2017/03/08/technology/snap-makes-a-bet-on-the-cultural-supremacy-of-the-camera.html

Mead, Rebecca. 2017. "The Prophet of Dystopia." *New Yorker*, April 17, 2017.

Pai, Tanya. 2017. "The Squishy, Sugary History of Peeps." *Vox*, April 11, 2017. http://www.vox.com/culture/2017/4/11/15209084/peeps-easter

In-text citation

(Manjoo 2017)

(Mead 2017, 43)

(Pai 2017)

For more examples, please consult The Chicago Manual of Style.

SCIENTIFIC EVALUATION PROCESS is developed according to the principle *double blind peer review*, by university teaching staff and scientific researchers with expertise in the field of the article. The author's identity is not known by evaluators and the name of the evaluators is not made known to authors.

Authors are informed of the conclusions of the evaluation report, which represent the argument for accepting/rejecting an article.

Consequently to the evaluation, there are three possibilities:

a) the article is accepted for publication as such or with minor changes;

b) the article may be published if the author makes recommended improvements (of content or of linguistic nature);

c) the article is rejected.

Previous to scientific evaluation, articles are subject to an *antiplagiarism analysis*.

DEADLINES:

All authors will send their articles in English to the editor's e-mail address, **impactstrategic@unap.ro**.

We welcome articles all year round.

NOTA BENE:

Authors are not required any fees for publication and are not retributed.

By submitting their materials for evaluation and publication, the authors acknowledge that they have not published their works so far and that they possess full copyrights for them.

Parts derived from other publications should have proper references.

Authors bear full responsibility for the content of their works and for ***non-disclosure of classified information*** – according to respective law regulations.

Editors reserve the right to request authors or to make any changes considered necessary. Authors give their consent to possible changes of their articles, resulting from review processes, language corrections and other actions regarding editing of materials. The authors also give their consent to possible shortening of articles in case they exceed permitted volume.

Authors are fully responsible for their articles' content, according to the provisions of *Law no. 206/2004 regarding good conduct in scientific research, technological development and innovation*.

Failing to comply with these rules shall trigger article's rejection. Sending an article to the editor implies the author's agreement on all aspects mentioned above.

For more details on our publication, you can access our site, http://cssas.unap.ro/en/periodicals.htm or contact the editors at impactstrategic@unap.ro

"CAROL I" NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE

Layout editor: Gabriela CHIRCORIAN

The publication consists of 170 pages.

"Carol I" National Defence University Printing House
Şoseaua Panduri, nr. 68-72, sector 5, Bucureşti
E-mail: editura@unap.ro
Tel: 021/319.40.80/215

Nr. 731/09.10.2024 C. 219/2024