BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

No. 2/ 2023

ISSN 2284-936X
eISSN 2284-9378

Publication founded in 1937

SCIENTIFIC PUBLICATION HIGHLY ACKNOWLEDGED IN THE FIELD OF "MILITARY SCIENCES, INFORMATION AND PUBLIC ORDER" OF THE NATIONAL COUNCIL FOR ATTESTATION OF ACADEMIC DEGREES, DIPLOMAS AND CERTIFICATES, INDEXED IN INTERNATIONAL DATABASES EBSCO, CEEOL, GOOGLE SCHOLAR, INDEX COPERNICUS, PROQUEST, DOAJ & ERIH PLUS

"CAROL I" NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE
BUCHAREST, 2023

The articles published in the Bulletin of "Carol I" National Defence University, ISSN 2284-936X, L 2284-936X, are also found – title, author, abstract, content and bibliography – in the Romanian version of the journal, ISSN 1584-1928.

Content

No. 2/2023

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY
https://buletinul.unap.ro/index.php/en/

The impact of Russia's aggresion on reshaping tomorrow's world

Ukraine's future scenarios, developments, and options

Assoc. Prof. Iulian CHIFU, Ph.D.*

*"Carol I" National Defence University, Bucharest, Romania
e-mail: keafuyul@gmail.com

Abstract

Prospective scenarios (Chifu 2022) are now piling up, on the eve of **Ukraine's announced counter-offensive** to reclaim its territories and create clear strategic advantages in the perspective of any negotiations with Russia (Menon 2023). While **the criteria and indicators** of short and medium-term development are easier to determine, as is the **aspirational goal of Ukraine to gain all its occupied territories** (Wallander 2023), there are numerous **inflection points** that may emerge, just as a number of **game-changers** are looming, elements that would radically change the reality and the course of the known trend. Taking these factors into consideration, we have drafted an updated outline of **Ukraine's potential future developments, scenarios, and options** in the event of a Russian full-scale war of aggression. It is important to note that these developments not only impact Ukraine but also have implications for the post-war global landscape.

Keywords:
prospective scenarios; indicators; inflection points; game changers.

Russia's war of aggression in Ukraine: Prospective studies. Prospective scenarios

Prospective studies (Chifu 2013, 167-186) are a specific type of future studies that implies identifying critical indicators, tipping points, inflection points, and relative certainties to build up scenarios on **short, mid and long term** with **continuity, discontinuity, and black swan possibilities** in order to cover a known possible evolution of a specific event, area, and phenomenon. This methodology aims to avoid strategic surprises and keep decision-makers in line with possible evolutions (Chifu 2014, 174).

The world has evolved from a **bipolar world** during the Cold War to a somewhat **globalized world, interdependent and driven by the market economy.** The 9.11 attack, terrorism in Europe and the West, the Color Revolutions, the Arab Spring, the pandemic, and the emergence of social media as well as other disruptive technologies **brought changes to the international order**, but without a dramatic change (more a transformational change) without establishing **where the transition period leads our world**. Now, Russia's aggressive war of attrition in Ukraine has transformed into a prolonged conflict and poses a significant threat to dramatically alter the landscape.

We maintain our position (Chifu 2022) that the future of the 21st century world marks a **dispersion and dissipation of power** as a result of new technologies and the scarce resources required for them, which makes the **leap already identified** from the two superpowers of the Cold War through the uni-multipolarism of the transition era to the **two great power system, none of them being Russia, and numerous regional powers**, with the perspective of a China-US rivalry that could fall into war. But above all, we are contemplating a more democratic world in which niches of power or resources can overnight transform **a state, however small, into a relevant power** in terms of resources or technology (Chifu 2021a; Chifu 2021b, 100-113) it possesses, and which are needed by the whole world.

In the case of Ukraine, the context established the **red lines of the West** related to the transfer of technologies. **Using military means by Russia** in the mid of the 21st century is unacceptable, but, at the same time, the support for the aggressed democratic country, Ukraine in that context, **should not break international law**, and create **escalation patterns**; on the contrary, it should just help Ukraine defend its territory and its citizens. This means **no Western boots on the ground**. This also means that the weapons delivered to Ukraine should be **proportional to the Russian attacks on its territory** and the range of those weapons should not allow Ukraine **to attack targets on the territory of Russia** (so outside its own territory) (U.S. European Command 2023).

This does not mean that the US or any other state **will prevent Ukraine from developing its strategies** with strikes outside its national territory, including in Russia.

Those strategies could also include **targeting weapons, groups of soldiers, railways, or fuel storage** outside of its borders, in an attempt **to break the supply lines of the aggressor**, but this should be done **with its own means**, with special operations forces and Ukrainian weapons, but not those transferred from other sources. Some of those Western weapons deliveries come explicitly with those **limitations**.

Key indicators and criteria for the evolution of Russia's war of aggression in Ukraine in the short and medium term

There are **four key conditions, indicators and criteria** that will define the evolution of Russia's war of aggression in Ukraine in the short and medium term, which we can place in a **3+1 format** depending on our **current ability to anticipate**:

- **The resilience of Ukraine and the Ukrainians**. The military capacity to resist on the front line, to lead the war effort, and the capacity of the population to sustain that effort in the long term. We have seen that the **morale and the will to fight** for a purpose matter first and foremost. The Ukrainians are defending their territory and their population as they are **fighting their real War of Independence** with the strongest motivation, while Putin has failed to produce a sustainable and credible narrative regarding **why he sent his troops into the Ukrainian territory** (continuing Putin's "Christmas tree" narrative that contains **in the mix Nazis, coup d'etat, defence of the Russians everywhere and countless other past things** about the cradle of the Russian state's birth or ignoring independence of the states and creating narratives of **state-civilizations** that would have oversized and dominant rights in relation to the neighbourhood, doomed to remain in their **sphere of influence**) (Russian Mission 2023). But equally important is **the effort behind the front** and the capacity to avoid attacks on cities and civilians. As long as the fighters in the first line know their families are safe, they can fight less constrained than in the situation on which they learn daily of **new attacks on apartment blocks, streets, or offices** in towns far behind the front.
- **Western resilience in supporting Ukraine**. It is about public support for the war effort **directly**, through humanitarian aid, export corridors, military aid, and financial-budgetary aid to support the war, but also **indirectly**, through inflation, energy costs, and many other elements of influence. As long as the Western citizens can maintain this commitment, and **the resilience of the West is assured**, there remains a major element of **transforming the traditional defence industry into a war industry** with large-scale production, which all allies must develop in the perspective of this long, large-scale war, but also of a larger deterrence effort that may come shortly after the current war in Ukraine, in the Indo-Pacific (Ash 2023).
- **Ukraine's ability to absorb the Russian offensive and conduct its own successful counter-offensive**. Of course, Ukraine has demonstrated that it can absorb the spring offensive and the fighting in the front line at Vuhledar

and Bahmut showed **Russia's inability to generate substantial gains** even with huge losses of men and military capabilities. However, the mandatory point remains the forthcoming **Ukrainian counter-offensive** (Menon 2023) which must show penetration capability and **substantial strategic gains** that will break the front in two – South and East – and put solid and credible pressure on Crimea. Only then would there be the preconditions for Russia to wish, demand, and participate in serious negotiations. **A possible stalemate in Ukraine's offensive with limited gains and major losses** would enshrine the stagnation of the front and the inability of the parties to make further territorial gains through combat, with negative effects on the perspectives of the war.

- **Vladimir Putin's ability to maintain the vertical of power**. It is a condition we can anticipate in theory but cannot credibly substantiate for two reasons: **the opacity of Putin's system** and the conformity of the elites and group around him, and above all, the autocratic nature of the regime which **can implode at the slightest and most insignificant trigger** (Kolesnikov 2023). The lack of foresight does not mean that this indicator (+1) should be eliminated, on the contrary, **it can always determine the fate of the war**, at moments that are difficult to predict.

Scenarios of the end of a war. From the Western aspirational position to the alternatives on the ground

Russia's war of aggression has, as an aspiration aim, only one endgame for any democratic actor concerned with the rules-based world and the prospects of world realignment:

- **Russia must lose the war and Ukraine must win**. It is a legal and moral solution capable of strengthening the criteria of a **rules-based world**. Any half-measure would set **a precedent** whereby an aggressor state could take over pieces of its neighbours' territory after such a precedent, especially after the famous pleadings in the sphere of the **security-versus-territory** doctrine (Aarts 1999; Adler and Barnett 1998), questionable in the Middle East but **unacceptable in the post-Helsinki Europe**, after the commitment not to change borders by force and to recognise the sovereignty, territorial integrity and independence of every CSCE/OSCE and UN member state.
- **Russia must pay**. As countless analyses indicate, the lack of **post-Cold War costs** to Russia as the successor to the treaties of the former USSR has led to a **readiness to resort to war** to solve Russia's problems in international relations and satisfy its excessive levels of ambition. On the other hand, the question of the **costs imposed on Russia** includes payment for launching a war, payment for the reconstruction of Ukraine, individual and collective payment for **war crimes** and crimes against humanity, as well as for the **crime of aggression**, but also conceding guarantees that **Russia will never use the**

war as an alternative for its ambitions in international relations (we have precedents with Japan and Germany after the World War II, but the level of sophistication nowadays increased dramatically and we could find better options for weapons control and double use products and industries in order to grant Russia staying away from any type of aggression for the foreseeable future).

- **The states, companies and consultants who helped Russia circumvent the sanctions must pay**. Western citizens have taken on the multiple costs, revealed above, with the hope that their children and grandchildren will live even in a form of **imperfect democracy**, but at least one in which they have the right to choose. Not to live under an autocrat like Putin telling them **how to live and what to think, say, do**. That is why it is the responsibility of governments to identify the **war profiteers** enriched by war, individuals, companies, or states that are helping to circumvent sanctions and make them pay for this (Spektor 2023). This creates **the moral high ground** needed to demand public support in such confrontations in the future.

Of course, if these are the **goals and aspirational targets**, the evolution of Russia's war of aggression in Ukraine can take many forms. **Russia has not yet been defeated**; it possesses a significant population and military reserves that it can deploy in the war effort. Additionally, it has various capabilities, primarily from stockpiles, that are morally outdated but can assist Putin in **sustaining the war in the medium and long term**, thereby avoiding any admission of defeat. However, the fighting is almost entirely taking place on Ukrainian territory, where the destruction is also taking place, so **Russia and Putin can always claim some form of victory**. The alternatives would be:

- **Ukraine's complete victory in the war**. Liberation of the entire territory and claiming victory and independence from Russia with the gun in hand.
- **Strategic victory in the war followed by a negotiation in Ukraine's advantage**. With a **separation of the southern and eastern fronts** and serious pressure on Crimea, the elements of a relevant strategic victory in the war for Ukraine are in place. Any negotiation from this point can be advantageous and auspicious for Kiev.
- **Standstill: the inability of the Ukrainian offensive, loss of Western support/ insufficient support.** Fatigue, lack of resources, or sufficient Western capabilities and ammunition may indeed lead to a ***de facto*** **freeze in the conflict**, which would effectively turn into a long-term war of attrition, with **Russian/Ukrainian stop-and-go** moments and periodic resumption of offensives, but with modest advantages, and pushing developments towards a **Korean variant** (Haass and Kupchan 2023).
- **The Russian strategic victory (apparently) satisfying** – full conquest of Donbas, significant destruction of the Ukrainian army on the offensive, **full occupation of territories formally annexed by Russia,** and their

Russification. But there would never be peace here, because **there will always be the possibility of renewed conflict**, hence the need for a long-term commitment.

- **Russia's complete victory**, i.e. the achievement of all the original objectives of the invasion: change of power in Kiev, occupation of a large part of the territory, *de facto* or *de jure* seizure of Ukraine – becoming a second Belarus – or the independence of **the landlocked Little Ukraine**. All that remains in this case for its neighbours, whether post-Soviet or NATO member states, would be to ask themselves **who is next?** Sustainable peace is not possible under these circumstances (Miliband 2023).

Game changers. Prospects for the escalation of the Ukrainian conflict on a global scale

We have identified **three game changers** that, once they occur in Russia's war of aggression in Ukraine, would dramatically change both the situation on the ground and the outlook for the world of tomorrow. For sure there are more such possible scenarios, and we will suggest some others, with different levels of relevance. Most importantly, they would pave the **way for the escalation of the conflict globally**, drawing in forces and causing an expansion of the conflict **geographically, of its scope, as well as in strategic stakes**. This is a prospect that the US, NATO and the West as a whole has tried and is working hard to avoid. In this case, the three formulas would be: **the involvement of China in the conflict** (Fix and Kimmage 2023), **the direct involvement of NATO troops in the fighting in Ukraine** or **the launch of tactical nuclear weapons by Russia**. The three can be tied to each other and determine each other.

China's involvement in the conflict (Jones 2023)

At present, China provides **formal, declarative, political, economic, financial, and technological non-lethal support to Russia**. Dual-use and non-sanctions goods can mean support for Russia but **without Beijing taking on the costs of war** or providing **a steady supply line of weapons to Putin's Russia**. Yet, this may change, first through **covert arms transfers** and with the ambiguity of a credible denial of this direct involvement in the supply of lethal weapons, possibly by assuming the **transfer through intermediaries** of just components rather than easily identifiable Chinese weapons on the ground. But developments may even move towards **an open, publicly assumed transfer or full-scale supply line of lethal weapons to Russia**, which would bring a radical change in the situation on the ground (Kurtz-Phelan 2023). This does not mean that **Russia could automatically win the war**, but the delivery of lethal weapons by China is both a relevant turning point and **a possible game changer in the war**.

Western involvement, NATO, US, Coalition of the Willing in Ukraine

As we presented above, NATO, the US, and the West as a whole have placed their support for Ukraine in the key of **limiting direct intervention** or the **presence of its troops on the ground** – with the exception of mercenaries on their own account and, perhaps, trainers on specific missions on the ground. However, the prospect of a Ukrainian defeat or Chinese involvement in the conflict, or even worse, Russia's use of tactical nuclear weapons in Ukraine, may also **push it beyond this limit**, to avoid **the prospect of pushing the confrontation to NATO borders**. The West's explicit military involvement, in whatever form, of its own troops in Ukraine turns Russia's war of aggression in Ukraine into **the battle of the next century on Ukrainian soil**. The stake is raised significantly and **the defeat of Ukraine is assumed to be an important loss, but doubled by the defeat of the West** and the rules-based world order in front of revisionism, neo-imperialism and the world's autocracies. China's involvement in the conflict would directly transform the battle in Ukraine into the key **confrontation of systems, democracy versus autocracy** and the right of states to freely choose their system of government, i.e. it would permanently alter state sovereignty and territorial integrity as a principle in the absence of Western intervention in support of Ukraine (Kausikan 2023). **The perspective of abandoning Ukraine is conceptually unacceptable.**

Russia's use of nuclear weapons in war

This would be the most significant game changer in the state of international relations since the Second World War. **Russia's use of nuclear weapons** is an implicit admission of the conventional defeat of Ukraine, but also a **complete exit of Russia from the world system**, with major costs of real isolation from all states of the world. We would no longer be talking about the autocracy versus democracy rivalry, but about **an actor in the system, moreover, a permanent member of the Security Council, that has completely escaped all logic and control**. China, India and the states of the Global South would find it very difficult to support Russia in any way, its **expulsion from the Security Council and complete isolation** would be matched only by the effort to rescue Ukraine, which would receive all the support it needs, including the presence of NATO troops directly on the ground, **to liquidate the consequences of such a hit** and to obtain the liberation of its territory.

There could also be some **other significant changes**. To give just an example, a new front between Russia and the Global West somewhere else, from the territory of the Baltic states or in the post-Soviet space or in remote areas like, why not, Sudan. That would mean **a continuous escalation of the war Russia-West**, in geographic terms, at once.

All of these elements would directly affect the **developments in the 21st century world**. But also the forms of conflict management, the structure and security framework or even the **survival and cohesion formulas** of some states, primarily **Russia and Ukraine**. Moreover, they would primarily influence the rules, or lack of any rules, by which the international relations of states will evolve in the 21st century (Mazarr 2023). In this context, **the classical discussions of unipolarism, Sino-American bipolarism or multipolarism** claimed by Russia and China would be meaningless, as would the **temptation to come back and claim again spheres of influence** and move to new types of power games of the big players.

References

Aarts, Paul. 1999. "The Middle East: a region without regionalism or the end of exceptionalism." *Third World Quarterly* 20 (5): 911-925.

Adler, Emanuel, and Michael N. Barnett. 1998. *Security Communities.* Cambridge University Press.

Ash, Timothy Garton. 2023. "Postimperial Empire. How the War in Ukraine Is Transforming Europe, Foreign Affairs May/June 2023." *Foreign Affairs* 102, no.3. https://www.foreignaffairs.com/ukraine/europe-war-russia-postimperial-empire.

Chifu, Iulian. 2013. „Analiză prospectivă. Experienţa internaţională şi o abordare românească." *Revista Română de Studii de Intelligence,* no.10: 167-186.

—. 2014. *Prospectives on Ukraine Crisis. Scenarios for a mid-long term evolution.* București: Editura Institutului de Științe Politice și Relații Internaționale al Academiei Române.

—. 2021a. „Securitate tehnologică. Un nou domeniul de strictă actualitate a securității viitorului." *Infosfera,* no.2: 13-22.

—. 2021b. „Când tehnologia şi social media întâlnesc Covid-19. Relativizarea adevărului şi soarta social media." *Romanian Intelligence Studies Review,* nr. 25: 100-113.

—. 2022. *Studii prospective și metodologii alternative. Eșafodajul de securitate în secolul 21*. Vol. 3, *Reconfigurarea securității și relațiilor internaționale în secolul XXI*. București: RAO.

Fix, Liana, and Michael Kimmage. 2023. "How China Could Save Putin's War in Ukraine. The Logic—and Consequences—of Chinese Military Support for Russia." *Foreign Affairs.* https://www.foreignaffairs.com/china/how-china-could-save-putins-war-ukraine.

Haass, Richard, and Charles Kupchan. 2023. "The West Needs a New Strategy in Ukraine, A Plan for Getting From the Battlefield to the Negotiating Table,." *Foreign Affairs.* https://www.foreignaffairs.com/ukraine/russia-richard-haass-west-battlefield-negotiations.

Jones, Seth G. 2023. "America's Looming Munitions Crisis. How to Fill the Missile Gap." *Foreign Affairs.* https://www.foreignaffairs.com/united-states/americas-looming-munitions-crisis.

Kausikan, Bilahari. 2023. "Navigating the New Age of Great-Power Competition.Statecraft in the Shadow of the U.S.-Chinese Rivalry." *Foreign Affairs.* https://www.foreignaffairs.com/united-states/china-great-power-competition-russia-guide.

Kolesnikov, Andrei. 2023. "Putin's Second Front. The War in Ukraine Has Become a Battle for the Russian Psyche." *Foreign Affairs.* https://www.foreignaffairs.com/russian-federation/putins-second-front.

Kurtz-Phelan, Dan. 2023. "How to Avoid a Great-Power War. A Conversation With General Mark Milley." *Foreign Affairs.* https://www.foreignaffairs.com/podcasts/how-to-avoid-great-power-war-mark-milley.

Mazarr, Michael J. 2023. "Why America Still Needs Europe. The False Promise of an "Asia First" Approach." *Foreign Affairs.* https://www.foreignaffairs.com/united-states/why-america-still-needs-europe.

Menon, Rajan. 2023. "Ukraine's Best Chance. A Successful Offensive Could End the War With Russia." *Foreign Affairs.* https://www.foreignaffairs.com/ukraine/ukraines-best-chance.

Miliband, David. 2023. "The World Beyond Ukraine. The Survival of the West and the Demands of the Rest." *Foreign Affairs* 102, no.3. https://www.foreignaffairs.com/ukraine/world-beyond-ukraine-russia-west.

Russian Mission. 2023. "The Concept of Foreign Policy of the Russian Federation." https://russiaeu.ru/en/news/concept-foreign-policy-russian-federation.

Spektor, Matias. 2023. "In Defense of the Fence Sitters. What the West Gets Wrong About Hedging." *Foreign Affairs* 102, no.3. https://www.foreignaffairs.com/world/global-south-defense-fence-sitters.

U.S. European Command. 2023. "Statement of General Christopher G.Cavoli (Unclassified)." https://www.eucom.mil/document/42351/gen-christopher-g-cavoli-2023-posture-statement-to-the-hasc.

Wallander, Celeste A. 2023. "Opening statement, Office of the Secretary of Defense, before the 118-th Congress Committee of Armed Services,." https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/04.26.23%20Wallander%20Statement.pdf.

No.2/2023, APRIL-JUNE
https://doi.org/10.53477/2284-9378-23-17

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

The New Revolution in Language Learning: The Power of Artificial Intelligence and Education 4.0

Assoc. Prof. Ana-Maria CHISEGA-NEGRILĂ, Ph.D.*

*"Carol I" National Defence University, Bucharest, Romania
e-mail: anachisega@gmail.com

Abstract

This article explores the connection between artificial intelligence (AI) and language learning in the context of Education 4.0, highlighting how the former revolutionizes the latter with the introduction of emerging technologies and innovations in education. The article discusses how AI improves the processes of language learning through personalized learning experiences, interactive practice, and automated assessment. AI can be used to create diverse learning materials and immersive experiences that align with the principles of Education 4.0. When used correctly, AI can bring numerous benefits to language learning, such as increased efficiency, greater student engagement in the teaching-learning process, and the accessibility of content from anywhere and on any device. Additionally, it emphasizes the need to adopt Education 4.0 accompanied by the development of content that equips students with the necessary skills in the digital age. The article also highlights the importance of integrating AI and Education 4.0 in language learning to promote critical thinking, problem-solving skills, and digital literacy.

Keywords:
artificial intelligence; education 4.0; language learning; chatbots; machine learning.

Education 4.0 marks a paradigm shift in the field of education driven by the impact of emerging technologies and innovative approaches on the learning process. In the digital age, Education 4.0 plays a vital role in preparing students for the increasingly complex environment of the 21st century, due to its ability to foster the development of critical skills required by a workforce that must respond to the demands of an ever-changing job market. As automation and artificial intelligence reshape industries, Education 4.0 emphasizes the cultivation of specific skills, including the 4Cs: critical thinking, communication, collaboration, creativity, as well as problem-solving, and digital literacy (Marietta College 2016, 3). These skills are highly important for individuals who wish to adapt to the rapid changes in the job market and thrive in a technology-based world.

To modernize education, traditional learning models are being replaced with personalized learning experiences. Through the use of technology, students can access educational content tailored to their needs and learning styles, to enhance the efficiency of the teaching-learning process and make a notable leap forward from traditional eLearning programs.

In recent years, the partnership established between artificial intelligence (AI) and language learning has emerged as a promising frontier in education. As AI technologies continue to develop and refine at a rapid pace, they are making their way into education, significantly impacting how foreign languages are taught and learned. This article provides a brief overview of this partnership while highlighting the importance of AI in transforming language learning experiences.

Industry and Education 4.0

The term "Industry 4.0" was announced at the Hannover Fair event in 2011 (Qina, Liua, and Grosvenora 2016, 173) and originated from a strategic plan developed by the German government in collaboration with the Industry Science Research Alliance and Acatech in 2013 (Ellahi, Khan, and Shah 2019, 700). The concept of Industry 4.0, which refers to the integration of digital and physical systems in various industries, emphasizes the need for a corresponding transformation in education, known as Education 4.0. As the Fourth Industrial Revolution brings about rapid advancements in technology and automation, traditional educational models must evolve to equip learners with the skills and competencies required in the digital age.

Education 4.0 is an innovative educational framework designed to strategically integrate a range of competencies into the learning experience, aligning with the demands of Industry 4.0 (I.D. 4.0). This approach includes essential areas such as artificial intelligence (AI), the Internet of Things (IoT), simulation, among others. By incorporating these elements, Education 4.0 aims to equip students with the necessary skills and knowledge to thrive in a rapidly evolving technological landscape

(Chakraborty, et al. 2023, 2). It recognizes the importance of adapting education to meet the current requirements and challenges presented by Industry 4.0.

According to Bartolomé (Bartolomé, Castañeda, and Adell 2018, 2-3), two fundamental characteristics of Education 4.0 are personalization and flexibility, both of which offer numerous educational benefits. Digital tools and platforms provide learners with access to vast amounts of information, interactive and personalized learning materials, enabling students to tailor their educational experiences to their individual needs and learning styles. Online learning platforms, virtual classrooms, and educational apps further enhance flexibility by allowing individuals to engage in self-paced learning and break free from the constraints of time and location. Additionally, the incorporation of technologies like virtual reality, augmented reality, and artificial intelligence promotes engagement, creating immersive and interactive learning environments that deepen understanding and enhance creativity.

Furthermore, Education 4.0 places a special emphasis on the development of lifelong learning skills. In an era when new technologies and industries emerge at a rapid pace, individuals must continuously update their skills and knowledge throughout their careers. Education 4.0 promotes a culture of lifelong learning, encouraging individuals to focus on continuous skill development to adapt to changes. Equally important is the promotion of critical thinking skills, which are essential for academic success and the transition to the job market (Almeida and Simoes 2019, 130). Education 4.0 aims to develop individuals' capacity to analyze, evaluate, and solve problems independently. By promoting critical thinking skills, Education 4.0 equips students with the tools necessary to navigate the complexities of the modern world and succeed in their academic pursuits and future careers (Marietta College 2016, 6).

Therefore, the emergence of Industry 4.0 would require a corresponding change in education towards an approach that focuses on developing skills and attitudes (Rus 2019, 338). Education 4.0 provides students with certain competencies needed in the society of the future through the integration of technology, the development of critical skills, and the promotion of lifelong learning. It prepares individuals to tackle the challenges and opportunities of Industry 4.0 and ensures their continued success in a constantly changing job market.

The Role of AI in Language Learning

The potential of artificial intelligence to replace humans in certain professions has raised concerns about job displacement (Lewis 2019, 32). To address this issue, individuals and education systems need to focus on lifelong learning because, in an ever-evolving job market, continuous learning is of paramount importance. Individuals should seek opportunities to acquire new skills and knowledge to adapt to the constantly changing job requirements and avoid becoming redundant. In this

context, teachers should use AI to assist people in achieving their learning goals, transforming it from an enemy to a partner, as in the not-too-distant future, almost everyone will be working with AI (Gleason 2018, 5).

The integration of artificial intelligence in language learning has immense potential to revolutionize the educational landscape for both learners and teachers. The emergence of AI-powered tools and platforms has opened up great possibilities in foreign language instruction. One significant advantage of AI in this context is its ability to analyze large amounts of data, enabling its algorithms to understand patterns of language usage, identify common errors, and provide detailed and tailored feedback to students. By using AI, students learning a foreign language can receive personalized information that meets their specific needs and preferences. This personalized approach offers a more efficient learning experience as students can focus on areas where they need more practice, receiving specific guidance designed for their needs (Redecker and Punie 2013, 8).

AI bears immense potential in language learning by offering innovative approaches that cater to the diverse needs and learning styles of individuals. Through AI, experiences in learning foreign languages can become more interactive, captivating, and aligned with how the new generation relates to technology and learns. AI-powered chatbots and virtual tutors can simulate real-life conversations and provide language practice anytime, on any device, and in the absence of a teacher. For example, they can assist in a persuasive writing exercise (Wambsganß, et al. 2021, 1) as well as in dialogues on various topics, correcting errors and offering translation support.

By using AI, language learners can access a multitude of resources, including online language courses, specialized platforms, and artificial intelligence programmed to provide support in a specific foreign language. These developments allow learners to take control of their learning and manage their linguistic skills on their own. With the help of AI technologies, educational platforms, and systems can better meet the needs of learners, offering personalized and adaptive learning experiences that align with their expectations and requirements (Pikhart 2021, 95-96).

AI holds great potential in transforming experiences in learning foreign languages as it can make them more personalized, interactive, and efficient, a characteristic that will certainly be refined in the future with the further development of AI. In the following sections, we will delve into more details on the various ways in which AI is revolutionizing language learning and explore their benefits and implications. This enables a more efficient and effective learning experience, as learners receive personalized instruction tailored to their individual needs and preferences a feature that was not supported by conventional learning (Mansor, Abdullah, and Rahman 2020, 443-444). AI can adapt to learners' progress by dynamically adjusting the difficulty level of exercises and providing relevant content to facilitate continuous improvement. Personalized and adaptive learning is a key feature facilitated by AI algorithms.

With the use of the AI, language learning platforms can deliver tailored content and experiences based on learners' proficiency levels, interests, and learning styles (Clarizia, et al. 2018, 291). As AI algorithms analyze learner data, they can adapt the learning materials and activities to optimize engagement and outcomes (Wambsganß, et al. 2021, 4). This personalized approach fosters greater learner motivation and increases the likelihood of successful language acquisition.

AI-based tutors and chatbots have brought a change in foreign language practice by allowing students to engage in conversation with AI tutors that simulate real-life scenarios, thus providing them with new opportunities to practice their written and oral communication skills. According to Haristiani (Haristiani 2019, 5), AI chatbots offer instant language practice and feedback with several advantages:

- Students feel more relaxed in conversations with a computer than with a person, and chatbots can repeat the same material endlessly with them without getting bored or being constrained by a location or a specific timeframe;
- AIs offer both text and synthesized speech, allowing students to practice their listening and reading skills, and providing them with a fresh and interesting experience;
- AIs also enable students to use a wide range of language structures and vocabulary that they would not typically have access to while providing quick and efficient feedback on spelling and grammar;
- AI tools such as chatbots provide a safe environment for students as they can practice without the fear of being judged; this type of interaction contributes to their confidence and fluency in the foreign language.

In addition, automated assessment and feedback on foreign language use are other important roles that AI can play in learning. AI technology can objectively assess learners' linguistic competence and provide automated feedback on grammar, pronunciation, and vocabulary usage. This instantaneous feedback allows learners to promptly identify and correct their mistakes, accelerating their progress in language learning (Wambsganss, et al. 2020, 4). AI-powered assessment systems that facilitate the evaluation process save time and resources for teachers while providing accurate evaluations of structures. However, some voices raise various concerns about the use of AI, particularly regarding the impact it can have on students' creativity through a number of limitations caused by the algorithms that govern it (Seo, et al. 2021, 14).

Conversational agents (CAs), such as Amazon Alexa or Google Assistant, can also provide significant support to students in their learning process, even though they were not specifically created for this purpose. One way in which teachers can use CAs is by implementing them as evaluation tools throughout a course. These CAs are widely accessible and user-friendly, even for teachers who do not have programming expertise, and by integrating CAs as evaluation tools during a course, teachers can gather valuable feedback on students' performance, particularly regarding speaking skills (Wambsganss, et al. 2020, 3).

Therefore, AI has become increasingly important in foreign language learning, offering access to personalized and adaptive learning, interactive practice through AI tutors and chatbots, and automated evaluation of grammar structures, pronunciation, etc. The integration of AI technologies into foreign language learning processes has a significant potential to improve both teaching efficiency and student engagement in the learning process. Importantly, students themselves show interest in using AI for learning, as they are already familiar with smart environments. Therefore, the incorporation of AI into various learning applications should not be ignored or neglected (Pikhart 2021, 95). As AI continues to advance, its role in foreign language learning is likely to expand, further transforming the educational landscape.

Benefits of AI in Language Learning

The integration of artificial intelligence in foreign language learning can bring numerous benefits, changing the way students develop language skills. Here are some key advantages of AI in foreign language learning:

- Personalized and adaptive instruction: Personalized learning encompasses four core elements: individual characteristics, individual performance, personal development, and adaptive adjustment. These elements are essential in tailoring the learning experience to the unique needs, abilities, and progress of each learner, providing a more efficient and personalized learning experience (Peng, Ma, and Spector 2019).
- Enhanced efficiency and accessibility: AI enables learners to access foreign language learning resources anytime and anywhere, at their own pace. Online platforms and mobile applications equipped with AI technologies offer a flexible and convenient learning experience, eliminating barriers of time and location.
- Intelligent language assessment: AI algorithms can accurately and objectively assess certain aspects of students' language proficiency. Through automated assessments, AI can evaluate their speaking, writing, listening, and reading skills, providing instant feedback on areas that need improvement. For example, automated essay scoring (AES) is a technology-driven process that uses AI algorithms to evaluate and assign scores to essays written by students. However, despite saving time and being reasonably accurate, AES still faces challenges in evaluating creativity, nuanced arguments, and contextual understanding. Despite these obvious challenges, researchers are actively working to improve AES by developing more sophisticated algorithms that capture subtleties and enhance contextual understanding (Ramesh and Sanampudi 2021, 2521-2522).
- Interactive language practice: AI-powered chatbots and virtual language tutors offer learners opportunities for interactive language practice. One of the advantages of chatbots as language-learning partners is their availability for continuous practice (Fryer, et al. 2020, 10). Unlike human conversation partners who may have limited availability, chatbots are available at any time,

providing learners with flexible and extended practice sessions. Students can confidently practice new language skills, experiment with different expressions, and strengthen their vocabulary and grammar (Fryer, et al. 2020, 12-13). This repetitive and interactive practice with a chatbot can significantly enhance language acquisition and proficiency, allowing learners to gain confidence and fluency in an accessible and user-friendly learning environment.

- Continuous learning and progress tracking: AI can track learners' progress over time and provide personalized recommendations for further study. By monitoring performance, AI algorithms can suggest learning materials and activities that help learners continuously improve their language skills. Effectively monitoring students' academic progress and identifying those in need of additional support are primary objectives for educational institutions. At the beginning of a course, it can be challenging for teachers to assess the individual capabilities and needs of their students (Khan, et al. 2021, 1). However, by utilizing artificial intelligence and other means, struggling students can be identified, and teachers can develop preventive or remedial measures tailored to their specific needs (Khan, et al. 2021, 2).
- Natural language processing and translation: AI-based natural language processing enables speech recognition and translation services. However, automatic analysis in foreign language learning can also be used to identify correctly formed linguistic structures, allowing for positive or negative feedback. To detect and diagnose learner errors, all approaches must include models that encompass the full range of variations, both correct and incorrect, that can occur within a specific activity and for a particular learner (Meurers 2021, 2). Thus, learners can benefit from real-time translation, pronunciation analysis, and language comprehension tools, in order to improve their language skills.

These advantages of artificial intelligence in foreign language learning provide students with personalized, efficient, and accessible instruction, enabling them to achieve their language learning goals. By harnessing the power of artificial intelligence, students can access interactive and tailored learning experiences that accommodate their individual needs and preferences.

AI-Driven Language Instruction and Resources

The use of AI in foreign language learning has allowed for the development of highly diverse materials that provide the interactivity that new generations are accustomed to. The advantage lies in the fact that AI algorithms can analyze a vast amount of linguistic data, enabling the creation of content that is more tailored to the needs and proficiency levels of students. These AI-powered resources offer interactive exercises and tests that promote active student engagement and provide greater control over the content, transforming the foreign language learning experience into a more dynamic and efficient one (Ramesh and Sanampudi 2021, 2521-2522).

The integration of AI tools has revolutionized many aspects of foreign language learning, such as speech recognition, pronunciation practice, and translation. AI-assisted speech recognition technology allows students to practice their speaking skills by providing precise feedback on pronunciation, intonation, and fluency. Students can engage in interactive speaking exercises and receive real-time evaluations, helping them perfect their pronunciation and develop authentic speech patterns (Fryer, et al. 2020, 12). One such AI-based application is Mondly, which offers interactive lessons, AI-powered conversations, vocabulary, and pronunciation development. The platform supports multiple languages, speech recognition, and exercises aimed at improving speaking, listening, reading, and writing skills. Mondly's program includes augmented reality lessons, gamified learning, progress tracking, online and offline access, and a variety of theme-based lessons to expand vocabulary (Mondly 2023).

A very useful tool, which can also be based on AI, is the one that provides text translation in different languages, allowing students to easily understand the provided materials or create new materials themselves. These tools use algorithms to provide the most accurate translations possible, enabling students to translate texts in real-time or correct their own texts using AI-powered models to improve their writing, reading, and comprehension skills.
In addition, another significant role played by AI is in creating immersive language learning environments using virtual and augmented reality technologies, which, together with AI algorithms, provide students with the opportunity to familiarize themselves with simulated contexts in a foreign language. Through virtual scenarios, students can practice their language skills in real-life situations, even if simulated with the help of AI, such as going shopping, having a conversation with a doctor, ordering food at a restaurant, making a hotel reservation, etc., or engaging in guided conversations with a virtual character. Additionally, AI can generate real-time feedback and diverse responses tailored to the conversation, allowing students to improve their language skills. AI algorithms will analyze the students' responses and provide personalized recommendations for additional practice, highlighting areas that need improvement and suggesting ways to achieve it.

In conclusion, AI-based language instruction and resources have already transformed the landscape of language learning by developing interactive learning materials, integrating AI tools for voice recognition, pronunciation practice, and translation, as well as creating immersive language learning environments. As AI continues to advance, its role in language learning will also evolve, providing personalized language instruction and helping students achieve their learning goals.

Ethical Considerations and Challenges

Even if AI-based tools are extremely useful in many fields, ethical problems and challenges may still arise when AI is integrated into foreign language learning.

Addressing potential biases and limitations is crucial to ensure fair and inclusive learning experiences, and language models should be designed to detect and modify biases present in the data used. Data privacy and security are also extremely important in AI-assisted platforms, as students' personal information needs to be protected through the implementation of strict regulations and security measures. Therefore, while AI plays an important role in foreign language learning, maintaining a balance between AI utilization and human interaction is essential, as human teachers are indispensable when it comes to understanding cultural context, and linguistic nuances, assessing creativity, and facilitating real-world communication.

AI-assisted language platforms collect and analyze a large amount of data about students, raising concerns regarding data privacy and security, as well as the policy changes needed in this context (Tuomi 2018, 7). Students should have control over their personal information and be informed about how their data is collected, stored, and used. Foreign language learning platforms must adhere to strict data protection regulations and implement robust security measures to protect students from unauthorized access or misuse. Therefore, transparent privacy policies and user consent mechanisms should be rigorously implemented to protect students from data breaches and other unpleasant incidents associated with working in the virtual environment.

AI is often considered as an unbiased tool for assessing student learning because it can easily rank them based on the input or data obtained from testing. However, sometimes test results may not accurately reflect the students' learning, as they do not take into account numerous aspects that AI cannot handle, such as critical thinking or problem-solving skills. While AI assessment tools provide insights and facilitate the grading process, a comprehensive evaluation framework that includes diverse forms of assessment is crucial because test scores alone may not adequately capture the students' actual level of proficiency (Tuomi 2018, 32). Thus, a holistic approach provides a more comprehensive view of their knowledge and skills.

Although AI can enhance foreign language learning experiences, it is essential to strike a balance between AI-driven instruction and human interaction. Foreign language learning is a complex and social process that benefits from human interaction, cultural nuances, and real-world communication. AI can support and complement language instruction, but it should not replace the role of human teachers and mentors, as it is much more beneficial for both AI and human teachers to work together in close collaboration (Seo, et al. 2021, 2). Incorporating opportunities for authentic human interaction, such as group discussions, human conversation partners, or language exchange programs, allows students to develop real-world communication skills, cultural understanding, and the ability to navigate authentic language contexts.

Educational institutions and foreign language learning platforms should, therefore, consider the pedagogical implications of AI integration, ensuring that students

receive a holistic learning experience that combines the benefits of AI-based resources with the guidance and expertise of human instructors, who are responsible for creating a balanced and effective learning environment.

Conclusion

This article has explored the role of AI in language learning and highlighted its potential to transform the way we teach and learn languages. Through AI-driven language instruction and resources, students can benefit from personalized and interactive learning materials, speech recognition tools, pronunciation practice, translation assistance, and immersive language learning environments. Thus, the advantages of AI in learning seem to be numerous, as this approach offers improved efficiency, instruction tailored to students' needs, and the system's ability to analyze large amounts of language data.

However, it is extremely important to consider the ethical considerations and challenges associated with AI in language learning. Addressing potential biases, ensuring data privacy and security, and maintaining a balance between the role of AI and human interaction and instruction are key factors in creating safe language learning experiences.

Using AI allows students to receive personalized instruction that meets their individual needs, while teachers receive valuable information to help improve their teaching methods. To fully utilize the benefits of AI in language learning, both teachers and policymakers, as well as students, need to adapt to the requirements of the new virtual landscape governed by AI. This involves promoting lifelong learning and intercultural skills and stimulating collaboration between humans and AI. With AI as a tool in language education, we can enhance the learning experience, effectively develop language skills, and prepare students for the challenges of globalization and the technology-based society.

References

Almeida, Fernando, and Jorge Simoes. 2019. "The Role of Serious Games, Gamification and Industry 4.0 Tools in the Education 4.0 Paradigm." *Contemporary Educational Technology* 10 (2): 120-136. doi:hpps://doi.org/10.30935/cet.554469.

Bartolomé, Antonio, Linda Castañeda, and Jordi Adell. 2018. "Personalisation in educational technology: The absence of underlying pedagogies." *International Journal of Educational Technology in Higher Education, 15(14)* 1-17. doi:https://doi.org/10.1186/s41239-018-0095-0.

Chakraborty, S., Gonzalez-Triana Y., Mendoza J., and Galatro D. 2023. "Insights on mapping Industry 4.0 and Education 4.0." *Front. Educ.* 8:1150190: 1-19. doi:https://doi.org/10.3389/feduc.2023.1150190.

Clarizia, Fabio, Francesco Colace, Marco Lombardi, Francesco Pascale, and Domenico Santaniello. 2018. "Chatbot: An Education Support System for Student." Editor A., Pop, F., Ficco, M., Palmieri, F. Castiglione. *Cyberspace Safety and Security. CSS 2018. Lecture Notes in Computer Science().* Amalfi: Springer, Cham. 291-303. doi:https://doi.org/10.1007/978-3-030-01689-0_23.

Ellahi, Rizwan Matloob, Moin Uddin Ali Khan, and Adeel Shah. 2019. "Redesigning Curriculum in line with Industry 4.0." *The 2nd International Conference on Emerging Data and Industry 4.0.* Leuven: Elsevier B.V. 699–708. doi:https://doi.org/10.1016/j.procs.2019.04.093.

Fryer, Luke K., David Coniam, Rollo Carpenter, and Diana Lăpușneanu. 2020. "Bots for language learning now: Current and future directions." *Language Learning & Technology* 24 (2): 8-22. http://hdl.handle.net/10125/44719.

Gleason, Nancy W. 2018. "Introduction." În *Higher Education in the Era of the Fourth Industrial Revolution*, de Nancy W. Gleason, 1-12. Singapore: Palgrave Macmillan. doi:https://doi.org/10.1007/978-981-13-0194-0_1.

Haristiani, Nuria. 2019. "Artificial Intelligence (AI) Chatbot as Language Learning Medium: An inquiry." *Journal of Physics: Conference Series.* Padang: IOP Publishing. 1-7. doi:10.1088/1742-6596/1387/1/012020.

Jian Qina, Ying Liua, and Roger Grosvenora. 2016. "A Categorical Framework of Manufacturing for Industry 4.0 and Beyond." *The Sixth International Conference on Changeable, Agile, Reconfigurable and Virtual Production.* Elsevier B.V. 173-178. doi:https://doi.org/10.1016/j.procir.2016.08.005.

Khan, Ijaz, Abdul Rahim Ahmad, Nafaa Jabeur, and Mohammed Najah Mahdi. 2021. "An artificial intelligence approach to monitor student performance and devise preventive measures." *Smart Learning Environments* (Springer) 8: 1-18. doi:https://doi.org/10.1186/s40561-021-00161-y.

Lewis, Pericles. 2019. "Globalizing the Liberal Arts: Twenty-First-Century." În *Higher Education in the Era of the Fourth Industrial Revolution*, de Nancy W. Gleason, editor N. Gleason, 15-38. Singapore: Palgrave Macmillan. doi:https://doi.org/10.1007/978-981-13-0194-0_2.

Mansor, Nor Azah, Natrah Abdullah, and Hayati Abd Rahman. 2020. "Towards electronic learning features in education 4.0 environment: literature study." *Indonesian Journal of Electrical Engineering and Computer Science* 19 (1): 442-450. doi:10.11591/ijeecs.v19.i1.pp442-450.

Marietta College. 2016. "Partnership for 21st century skills – core content integration." https://www.marietta.edu/sites/default/files/documents/21st_century_skills_standards_book_2.pdf.

Meurers, Detmar. 2021. "Natural Language Processing and Language Learning." Cap. Natural Language Processing and Language Learning în *Concise Encyclopedia of Applied Linguistics*, de Carol A. Chapelle, 1-16. Wiley-Blackwell. https://www.wiley.com/en-sg/The+Concise+Encyclopedia+of+Applied+Linguistics-p-9781119147367.

Mondly. 2023. https://www.mondly.com.

Peng, Hongchao, Shanshan Ma, and Jonathan Michael Spector. 2019. "Personalized adaptive learning: an emerging pedagogical approach enabled by a smart learning environment." 331767551_Personalized_Adaptive_Learning_An_Emerging_Pedagogical_Approach_Enabled_by_a_Smart_Learning_Environment.

Pikhart, Marcel. 2021. "Human-computer interaction in foreign language learning applications: Applied linguistics viewpoint of mobile learning." Edited by Ansar Yasar Elhadi Shakshuki. *Procedia Computer Science.* Warsaw: Elsevier BV. 92-98. doi:https://doi.org/10.1016/j.procs.2021.03.123.

Ramesh, Dadi, and Suresh Kumar Sanampudi. 2021. "An automated essay scoring systems: a systematic literature review." *Artificial Intelligence Review* 55: 2495–2527. doi:https://doi.org/10.1007/s10462-021-10068-2.

Redecker, Christine, and Yves Punie. 2013. "The Future of Learning 2025: Developing a vision for change." *Future Learning* 2 (1): 3-17. doi:10.7564/13-FULE12.

Rus, Dana. 2019. "Creative Methodologies in Teaching English for Engineering Students." Editor George-C. Vosniakos. *Procedia Manufacturing.* Athens: Science Direct. 337-343. doi:https://doi.org/10.1016/j.promfg.2020.03.049.

Seo, Kyoungwon, Joice Tang, Ido Roll, Sidney Fels, and Dongwook Yoon. 2021. "The impact of artificial intelligence on learner–instructor interaction in online learning." *Int J Educ Technol High Educ* 18: 1-23. doi:https://doi.org/10.1186/s41239-021-00292-9.

Tuomi, Ilkka. 2018. "The Impact of Artificial Intelligence on Learning, Teaching, and Education. Policies for the future." Luxembourg: Publications Office of the European Union, 1-47. doi:10.2760/12297 (online).

Wambsganss, Thiemo, Rainer Winkler, Matthias Söllner, and Jan Marco Leimeister. 2020. "A Conversational Agent to Improve Response Quality in Course Evaluations." *CHI EA '20: Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems.* Honolulu: ACM. 1-9. doi:DOI: 10.1145/3334480.3382805.

Wambsganß, Thiemo, Tobias Kueng, Matthias Söllner, and Jan Marco Leimeister. 2021. "ArgueTutor: An Adaptive Dialog-Based Learning System for Argumentation Skills." *CHI Conference on Human Factors in Computing Systems.* Yokohama: ACM. 1-13. doi:https://doi.org/10.1145/3411764.3445781.

No.2/2023, APRIL-JUNE
https://doi.org/10.53477/2284-9378-23-18

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Revolutionizing space security: The Laser Patroller Satellite – A technological marvel of modern warfare

Eng. Ulpia Elena BOTEZATU, Ph.D.*
Eng. Victor VEVERA, Ph.D.**

*Romanian Space Agency; National Institute for Research & Developement in Informatics – ICI Bucharest, Romania
e-mail: ulpia.botezatu@ici.ro

**National Institute for Research & Developement in Informatics – ICI Bucharest, Romania
e-mail: victor.vevera@gmail.com

Abstract

This comprehensive article analyses the Laser Patroller Satellite (LPS) and its capabilities for enhancing security and safety in space exploration. The article is organized into five sections. Section 1 presents the context of the growing problem of space debris and the need for effective solutions. In Section 2, the features of the LPS, including its advanced sensors and tracking capabilities, are discussed. Section 3 elaborates on the capabilities of the satellite, such as space debris monitoring and tracking, space traffic management, debris removal, space situational awareness, and space exploration. Section 4 discusses the potential applications of the LPS in various areas, such as space debris mitigation, space security, and governance of space. Section 5 examines the implications of the LPS for international relations, including space policy, diplomacy, and governance. The article highlights the need for effective space governance frameworks to ensure the responsible and sustainable use of emerging technologies like the LPS, which raises concerns about privacy and the use of surveillance technology. In conclusion, the LPS is a powerful technology that has significant implications for space security, diplomacy, and governance, and it is crucial for nations to work together to develop policies that promote the responsible and sustainable use of space for the benefit of all.

Keywords:
Laser Patroller Satellite; space debris; space surveillance; space situational awareness; space governance; international cooperation.

The development of space technology has been rapidly advancing in recent years, enabling the creation of sophisticated satellites with a range of applications. One of these satellites is the Laser Patroller Satellite (LPS), a revolutionary system designed to provide enhanced surveillance and security capabilities in space. Its advanced laser technology enables the detection and tracking of moving targets from space, making it a powerful tool for national security agencies. The LPS is primarily developed to monitor space debris, a critical solution to the growing problem of space debris that poses significant threats to space operations and astronaut safety. As the international community continues to explore space and expand its presence in the cosmos, technologies like the LPS have become essential to ensuring the safety and security of space operations. This academic article provides a detailed analysis of the features, capabilities, potential applications, and implications of the LPS for international relations and space governance. The article aims to deepen the understanding of the technology behind the LPS and its contributions to revolutionizing space security and military technology.

The Laser Patroller Satellite represents a significant milestone in space technology and military advancements, with its innovative and sophisticated laser-based sensors that can detect, track, and monitor space debris with unprecedented precision. The deployment of the LPS marks a critical step toward space situational awareness, space traffic management, and space security (Finkleman 2010). With its advanced capabilities, the LPS can help to mitigate the risks posed by space debris and ensure the safety of space operations and astronauts (Stansbery 2021).

Moreover, the LPS has potential applications in the field of space warfare, where it can provide valuable support in detecting and tracking enemy satellites and other spacecraft (European Space Agency 2020). Its ability to provide real-time monitoring and situational awareness of space objects can provide critical intelligence for military operations. Furthermore, the LPS's advanced laser technology can be used for precise targeting and guidance of space-based weapons systems (Finkleman 2010).

However, the deployment and use of such technology also have significant implications for international relations and space governance (Johnson-Freese 2007). The use of space-based weapons and the development of technologies that enhance military capabilities in space can escalate tensions among nations and trigger arms races in space (Budning, Wilner and Cote 2021, 594-605; Hebert 2014). As such, international cooperation and collaboration are critical in ensuring the responsible and sustainable use of space for peaceful purposes.

This article aims to provide military audiences with an in-depth analysis of the Laser Patroller Satellite's technology, features, capabilities, and potential applications in military operations, as well as the implications of its deployment for international relations and space governance. By exploring the LPS's technological marvels and potential benefits and challenges, this article aims to deepen military audiences'

understanding of the critical role played by space technology in modern warfare and the importance of responsible space governance.

Space Debris: A Growing Threat to National Security and Space Operations

In recent years, the field of space technology has experienced significant advancements, which have led to the development of advanced satellites that serve a range of purposes (Botezatu 2021). One of the most critical challenges facing space exploration is the issue of space debris. As mentioned, space debris refers to any man-made object that orbits the Earth and is no longer functional. The accumulation of space debris has been a growing concern for space agencies worldwide due to the potential danger it poses to operational spacecraft and the safety of astronauts. Collisions between spacecraft and debris can result in significant damage, and the risk increases as the amount of space debris continues to grow.

Space debris is a significant challenge that requires urgent attention and intervention, particularly as the number of objects in space continues to increase. According to recent estimates, there are currently over 9,000 tons of space debris orbiting the Earth, with roughly 34,000 objects larger than 10 cm in diameter and millions of smaller fragments (The European Space Agency n.d.; Association of Space Explorers 2020). The accumulation of space debris has become a major concern for space agencies worldwide, and efforts are underway to reduce the risks it poses to space operations and safety (Botezatu and Piso 2020, 329-336).

Various strategies have been proposed to address the problem of space debris, including debris removal and mitigation measures, such as limiting the creation of new debris and reducing the risk of collisions (NASA 2021). However, these strategies require accurate and reliable data on the location, trajectory, and characteristics of space debris (Valsecchi and Rossi 2002). This is where the Laser Patroller Satellite comes in, as it offers a powerful solution to the problem of space debris through its advanced laser technology and high-resolution imaging capabilities.

To address this problem, scientists have developed a range of techniques and technologies aimed at detecting and tracking space debris. The Laser Patroller Satellite is one such technology that uses advanced laser technology to detect and track space debris, making it a powerful tool for space situational awareness and management (Schall 1991). The development of the Laser Patroller Satellite is part of ongoing efforts to mitigate the risks posed by space debris and ensure the safety of space operations. Through this article, we aim to provide an in-depth analysis of the Laser Patroller Satellite and its potential applications for enhancing security in modern times.

In addition to space debris management, the Laser Patroller Satellite also has significant implications for national and international security. Its advanced capabilities can be used for a range of applications, including intelligence gathering, threat detection, and military surveillance. However, the use of space-based technologies for military purposes raises important ethical and legal questions, and there is a need for international cooperation and regulation to ensure the responsible and peaceful use of space. The Laser Patroller Satellite represents a significant technological achievement, but its use must be carefully managed to prevent any potential negative consequences for global security.

Laser Patroller Satellite's Advanced Features for Enhanced Security

This section focuses on the Laser Patroller Satellite and its various advanced functions. LPS is a compact satellite equipped with advanced laser technology that allows it to detect and track moving objects on the Earth's surface. It is designed to operate in low Earth orbit, providing real-time surveillance of specific areas. LPS can be easily repositioned to cover different areas of interest, making it extremely versatile for security agencies.

Laser Patroller Satellite is designed as a space laser weapon that can defend against airborne threats (Syed, Mujahid and Syed 2021). The technology behind this satellite involves the use of a powerful laser beam to destroy or disable the target by overheating or disrupting its electronics. This satellite operates from space, allowing it to respond quickly to any threat and provide great flexibility and mobility in a changing battlefield (Schall 1991). It works in tandem with other space and ground-based defence systems to provide comprehensive and layered defence against hostile actions.

The Laser Patroller Satellite uses advanced laser technology capable of detecting and tracking even the smallest space debris. The satellite uses a laser ranging system that emits a laser beam towards the target object (Shen, Jin and Hao 2014). The laser beam is reflected back to the satellite, where it is analyzed to determine the location and trajectory of the object. Furthermore, the satellite is equipped with a LIDAR system that uses laser pulses to create a 3D map of the surrounding space (Fix, et al. 2019). This system provides a detailed image of the location and movement of space debris, allowing operators to accurately predict potential collisions.

In addition, the Laser Patroller Satellite is equipped with high-resolution cameras that capture images of space debris (Schall 1991). These images provide valuable information about the size, shape, and orientation of the debris, which can be used to determine the origin and potential impact of the object. Moreover, the Laser Patroller Satellite is designed to operate autonomously, allowing it to detect and track

space debris without human intervention (Klinkrad 2023). The satellite's onboard computer analyses data in real-time, allowing it to make decisions and adjust its trajectory to avoid potential collisions.

Furthermore, the LPS's ability to work in concert with other space and ground-based defence systems provides comprehensive and layered defence against hostile actions. In the event of an incoming threat, the satellite can quickly respond from space with its high-powered laser beam, providing a high degree of flexibility and mobility in a rapidly changing battlefield. The Laser Patroller Satellite can also be used to monitor missile launches and track their trajectories, providing early warning of potential attacks (Zhang, et al. 2020).

The Laser Patroller Satellite is not only a powerful tool for detecting and monitoring space debris, but it is also an effective weapon against hostile actions. Its advanced laser technology, along with its autonomous operation and real-time data analysis capabilities, make it a reliable and effective solution for space defence. Moreover, the Laser Patroller Satellite is highly versatile and can be used for a wide range of applications, including environmental monitoring, disaster response, and search and rescue operations. Its ability to quickly reposition and track targets makes it an ideal tool for responding to natural disasters such as hurricanes, earthquakes, and wildfires. The LPS can also be used to track the movement of ships and aircraft, providing valuable information for maritime security and air traffic control.

In conclusion, the Laser Patroller Satellite is a groundbreaking technology that leverages advanced laser technology to detect and monitor space debris and defend against aerial threats. Its exceptional capabilities, including autonomous operation, laser ranging system, LIDAR system, and high-resolution imaging, make it a powerful tool for ensuring the safety and sustainability of space operations. With its versatility and effectiveness, the Laser Patroller Satellite is a valuable asset for national security agencies, disaster response teams, and other organizations involved in space operations.

The Potential Applications of the Laser Patroller Satellite

The Laser Patroller Satellite (LPS) offers a range of potential applications beyond its primary function of detecting and monitoring space debris (Papadimitriou, et al. 2019). Its advanced capabilities make it a valuable tool for a variety of security and law enforcement applications (Zhao, et al. 2022). The following are some of the potential applications of the LPS:

Border control: The LPS can be used to monitor borders and detect illegal activities such as drug trafficking and smuggling. Its high-resolution imaging system can capture detailed images of the ground from space, allowing security agencies to monitor potential threats and respond quickly.

The Laser Patroller Satellite can be used to enhance border control efforts by providing real-time intelligence on the movement of people and vehicles. With its high-resolution imaging system and laser technology, the satellite can detect and track moving targets, including vehicles, ships, and aircraft, from space (Słomczyńska and Frankowski 2016). This capability can be especially valuable for monitoring remote or hard-to-reach areas, where traditional methods of border control may be limited. The satellite's ability to operate autonomously is particularly useful for border control applications. It can detect and track suspicious activity without human intervention, providing early warning of potential security threats (SSPI Association 2022). The onboard computer system analyses data in real-time, allowing the satellite to make decisions and adjust its trajectory as needed to monitor potential threats.

Moreover, the Laser Patroller Satellite's high-resolution imaging system can provide detailed images of the ground, including topography, infrastructure, and vegetation. This information can be used to identify potential crossing points, smugglers' routes, and other security risks along the border (Oliveira Martins, Lidén and Jumbert 2022). The satellite can also be used to support law enforcement agencies by tracking suspects or monitoring criminal activity. Its ability to detect and track moving targets from space can be used to identify suspicious behaviour and track the movements of individuals or vehicles of interest. This information can be combined with other intelligence sources to build a comprehensive picture of criminal activity (Wei and Yang 2021, 101-154).

Overall, the Laser Patroller Satellite is a highly versatile technology with a wide range of potential applications for border control. Its ability to detect and track moving targets autonomously, high-resolution imaging system, and laser technology make it a valuable asset for enhancing border security and monitoring potential security threats.

Maritime surveillance: The LPS's ability to detect and track moving targets, including ships, makes it a valuable asset for maritime surveillance. It can provide data on the speed, direction, and trajectory of these targets, allowing security agencies to monitor potential threats and respond quickly (Wei, Zhang and He 2021). Maritime surveillance is another potential application of the Laser Patroller Satellite (LPS). As the LPS has the capability to detect and track moving targets, it can be used to monitor the movement of vessels on the open seas, including illegal activities such as smuggling and piracy. The satellite's ability to track small vessels in real-time and monitor their movements can help enhance maritime security and prevent illegal activities.

The LPS can also be used to monitor and protect sensitive areas such as ports, coastlines, and offshore installations. It can detect and track vessels that may be approaching or loitering in restricted areas, providing early warning to security forces. This can help prevent unauthorized access to sensitive locations and improve the overall security of the maritime environment. In addition, the LPS can also

https://doi.org/10.53477/2284-9378-23-18

support search and rescue operations at sea. It can detect distress signals and provide real-time location information, enabling rescue teams to respond quickly and efficiently to emergencies.

Overall, the LPS's capability for maritime surveillance has significant potential for enhancing maritime security and safety. It can improve the effectiveness of maritime law enforcement, enable more efficient search and rescue operations, and contribute to the protection of vital maritime infrastructure.

Disaster response: The LPS can also be used to assist in disaster response efforts by providing real-time information on the location and extent of natural disasters, such as hurricanes and earthquakes. This information can be used to coordinate relief efforts and provide early warning to affected populations. The Laser Patroller Satellite can also be utilized for disaster response operations. During natural disasters such as hurricanes, tsunamis, and earthquakes, communication infrastructure on the ground may be destroyed, making it difficult for rescue teams to communicate and coordinate their efforts. In such scenarios, the Laser Patroller Satellite can act as a communication relay, providing a reliable and uninterrupted means of communication for rescue teams in affected areas.

Moreover, the satellite can provide critical information about the extent of the damage and the location of survivors, enabling rescue teams to prioritize their efforts and optimize their rescue operations. The LPS can also detect potential hazards such as landslides, mudslides, and flooding, allowing rescue teams to adjust their strategy and ensure their safety while conducting operations. By leveraging the LPS's advanced capabilities, disaster response teams can operate more effectively and efficiently, which can ultimately save lives and minimize damage.

Research studies have demonstrated the potential of satellite technology, including the use of Synthetic Aperture Radar (SAR) and other remote sensing techniques, in disaster response and emergency management. For example, a study conducted by researchers at the University of Tokyo explored the use of SAR data for monitoring and assessing damage caused by the 2011 Tohoku earthquake and tsunami in Japan (Gokon, et al. 2014). Another study conducted by researchers at the University of California, Los Angeles (UCLA) investigated the use of SAR data for mapping the damage caused by Hurricane Harvey in Houston, Texas in 2017 (Scotti, Giannini and Cioffi 2020). These studies demonstrate the potential of satellite technology for disaster response and emergency management.

Conflict monitoring: The LPS can be used to monitor areas of conflict or tension, providing valuable intelligence to security agencies. Its ability to detect and track moving targets from space makes it a valuable asset for law enforcement agencies, enabling them to track suspects or monitor suspicious activity.
The Laser Patroller Satellite can also be used for monitoring areas of conflict or

tension. The satellite's high-resolution imaging capabilities and ability to detect and track moving targets from space make it a valuable asset for security agencies, enabling them to monitor suspicious activities and track suspects. In conflict zones, the satellite can provide real-time information on troop movements, weapons deployments, and other activities that could pose a threat to security. This information can be used to enhance situational awareness, enable early warning of potential threats, and inform decision-making by military and security personnel.

The Laser Patroller Satellite's conflict monitoring capabilities can also help prevent the escalation of conflict by enabling security agencies to detect and respond to potential threats before they escalate into full-blown conflicts. This can help save lives and prevent the destruction of critical infrastructure. Overall, the Laser Patroller Satellite's conflict monitoring capabilities can enhance the ability of military and security personnel to identify and respond to potential threats, prevent the escalation of conflict, and maintain peace and security in conflict-prone regions.

The Laser Patroller Satellite (LPS) is a promising technology that has the potential to revolutionize the way we monitor and manage space debris. As the amount of space debris continues to grow, there is an increasing need for effective solutions to mitigate its risks. The LPS is a unique tool that can detect and track space debris with unparalleled accuracy from space, making it highly effective in monitoring the movement of space debris, predicting potential collisions, and providing early warning to operational spacecraft.

Several academic studies have highlighted the importance of space debris monitoring and management. For instance, a study conducted by (Klinkrad 2006) identified the risks associated with space debris and the need for better monitoring and mitigation strategies. Similarly, a study by (Liou, Johnson and Hill 2014) emphasized the importance of space debris mitigation and provided recommendations for improving space debris management.

In addition to space debris monitoring and tracking, the LPS can also be used for space traffic management, debris removal, space situational awareness, and space exploration. These applications have been discussed in several academic studies. For instance, a study by (Johnson, Horri and Faber 2016) proposed using laser-based technologies, such as the LPS, for space debris removal. Similarly, a study by (Zhao, et al. 2017) proposed using laser communication technologies for space traffic management.

Overall, the LPS has the potential to address some of the most pressing challenges in space debris monitoring and management. Its ability to detect and track space debris with unparalleled accuracy makes it a highly effective tool for a range of space-related applications. As space activities continue to grow, the importance of the LPS in space monitoring and management is likely to increase.
In conclusion, the Laser Patroller Satellite is a highly advanced and versatile

technology with diverse applications, ranging from security to space exploration. Its unique ability to detect and track moving targets with unparalleled accuracy and efficiency makes it an indispensable tool for border control, maritime surveillance, and disaster response. Additionally, the LPS's potential for space-related applications, including space debris monitoring and tracking, space traffic management, debris removal, and space situational awareness, positions it as a critical technology for mitigating risks associated with space exploration and the rapidly growing amount of space debris. Overall, the Laser Patroller Satellite represents a significant advancement in satellite technology and holds great potential for addressing various challenges faced by military and space agencies alike.

Examining the Limitations and Risks of the Laser Patroller Satellite Technology

The Laser Patroller Satellite is a remarkable technology with many potential applications, but there are also limits and potential dangers associated with its use. One of the primary concerns is the possibility of using this technology for nefarious purposes, such as spying on civilians or engaging in aggressive military action. The development of this technology must be carefully monitored and regulated to ensure that it is used in ways that serve the common good and not just the interests of a particular nation or group.

Another important concern is the potential for the Laser Patroller Satellite to interfere with other satellite systems or to cause damage to spacecraft in orbit (Zhang, et al. 2021). This technology relies on the emission of high-powered lasers, which could potentially cause damage to other satellite systems or interfere with their operation. It is essential to carefully evaluate the potential risks and benefits of using this technology in different contexts to ensure that it is used safely and responsibly.

In addition to these concerns, there are also limits to the capabilities of the Laser Patroller Satellite. While it is an advanced technology with many impressive features, it is not a silver bullet solution for all security and space-related challenges. There may be other technologies or approaches that are better suited to particular contexts or challenges, and it is important to carefully evaluate the strengths and limitations of different approaches before deciding on a course of action.

Overall, while the Laser Patroller Satellite is a promising technology with many potential applications, it is essential to be aware of the potential limits and dangers associated with its use. Careful evaluation, regulation, and responsible use are necessary to ensure that this technology is used in ways that promote the common good and do not cause harm.

The Implications of the Laser Patroller Satellite for International Relations

Exploring the implications of the Laser Patroller Satellite for international relations reveals a complex set of issues that must be addressed. While the technology has the potential to contribute to global efforts to mitigate the risks of space debris and improve space safety, it could also raise concerns about the potential militarization of space and the use of surveillance technology. This section highlights some of the potential implications of the LPS for international relations, including space debris mitigation, space security, diplomatic relations, and the governance of space. As space activities become increasingly complex and crowded, it is essential for nations to work together to develop effective space governance frameworks that can ensure the responsible and sustainable use of space for the benefit of all.

Space debris mitigation

Space debris poses a significant threat to space missions and can cause damage to operational spacecraft. The Laser Patroller Satellite offers a promising solution for mitigating the risks of space debris by providing accurate and timely information on the location and movement of debris (Sormani, Bianco and Rossi 2016). This information can facilitate international cooperation on space debris removal and management, leading to a safer and more sustainable space environment. The deployment of the Laser Patroller Satellite could also enhance the effectiveness of current space debris monitoring systems and contribute to the development of new debris mitigation technologies.

The Laser Patroller Satellite's ability to track and monitor space debris with unprecedented accuracy makes it a valuable tool for space debris mitigation efforts. As a result, the technology could play a critical role in mitigating the risks of space debris and improving the safety and sustainability of space activities. Its deployment could also serve as a catalyst for international cooperation on space governance issues and facilitate the development of more effective space governance frameworks.

Space security

The Laser Patroller Satellite has significant implications for space security and the potential for its use to track and monitor other nations' spacecraft has raised concerns about the militarization of space. The use of the LPS for intelligence gathering and surveillance could lead to increased tensions between nations, particularly if it is used to monitor sensitive areas or activities. In addition, the potential for the LPS to be used for espionage or other nefarious purposes could also lead to security threats in space. While the LPS has the potential to enhance space situational awareness and provide valuable information on the movement of objects in space, it will be important for nations to consider the implications of its use and work together to establish clear rules and regulations to prevent its misuse.

The potential militarization of space and security threats associated with it have been a concern for the international community for decades (Hays 2020). The deployment of advanced technologies like the LPS further complicates the issue and raises questions about the potential for a new space arms race. Effective space governance frameworks that promote international cooperation and prevent the misuse of advanced space technologies will be essential in ensuring a secure and sustainable space environment for all.

Diplomatic relations

The development and deployment of the Laser Patroller Satellite could have significant implications for diplomatic relations between nations. The technology's advanced capabilities and potential for surveillance could be seen as a demonstration of technological prowess, potentially leading to concerns about a new space arms race. This could create tensions between spacefaring nations and affect international cooperation on space policy and governance (Weeden and Sampson 2020). However, the Laser Patroller Satellite also has the potential to be a positive development for international cooperation in space (Johnson-Freese 2021; Jakhu and Pelton 2021). By providing accurate and timely information on the location and movement of space debris, the LPS could contribute to efforts to mitigate the risks of space debris and improve space safety. Additionally, the technology could facilitate international cooperation on space governance issues, leading to more effective frameworks for the responsible and sustainable use of space resources (Dawson 2017).

The potential diplomatic implications of the Laser Patroller Satellite underscore the importance of considering the broader geopolitical context in which it is being developed and deployed. As space becomes more crowded and complex, there is a growing need for effective space governance frameworks that can ensure the safety and sustainability of space activities. By working together to develop such frameworks, nations can help ensure that the deployment of advanced technologies like the Laser Patroller Satellite contributes to the responsible and peaceful use of space resources for the benefit of all.

Governance of space

The governance of space is a crucial aspect of the peaceful and sustainable use of outer space. With the growing complexity and crowding of the space environment, there is a need for effective frameworks and mechanisms to ensure the safety and sustainability of space activities (Wiser and Timiebi 2023; Al Amiri 2023). The Laser Patroller Satellite has implications for space governance, as it represents a significant technological advancement that could contribute to the development of such frameworks.

The Laser Patroller Satellite's ability to provide accurate and timely information on the location and movement of space debris could be instrumental in mitigating the risks associated with space debris. This could help foster international cooperation

on space debris removal and management, which is vital for the safety and sustainability of space activities. Furthermore, the satellite's advanced surveillance capabilities could help in the monitoring of the space environment, enhancing the situational awareness of space actors and contributing to the development of effective governance frameworks.

However, as mentioned in the previous sections, the deployment of the Laser Patroller Satellite could also lead to concerns about the militarization of space and potential security threats. These concerns could exacerbate existing geopolitical tensions and affect diplomatic relations between nations. Therefore, it is essential to develop effective space governance frameworks that can balance the need for technological advancement with the importance of international cooperation, transparency, and responsible behaviour.

Overall, the Laser Patroller Satellite has significant implications for international relations, particularly in the realm of space policy and governance. It is crucial for nations to work together to develop effective space governance frameworks that can ensure the responsible and sustainable use of space for the benefit of all.

Conclusion

The Laser Patroller Satellite is a cutting-edge technology that presents an array of potential applications for national security agencies. The satellite's advanced laser technology has the capability to detect and track moving targets from space, making it a powerful tool for space situational awareness and management. However, the use of such advanced surveillance technology also raises concerns about privacy and the need for international cooperation on space governance and policy.

Despite these concerns, the Laser Patroller Satellite offers an innovative solution to the growing problem of space debris, which poses a significant risk to space exploration and safety. Its advanced capabilities for accurate tracking and monitoring of space debris and space traffic management make it a valuable tool for the international community in mitigating the risks of space debris and improving space governance.

As space technology continues to advance, it is crucial for nations to consider the implications of emerging technologies and work together to develop effective space governance frameworks that can ensure the responsible and sustainable use of space. The deployment of space-based systems like the Laser Patroller Satellite has significant implications for international relations, particularly in the realms of space security, diplomacy, and governance. Therefore, it is essential for nations to collaborate and develop effective policies and regulations that balance the benefits of space-based technologies with the need for international cooperation and responsible use of space for the benefit of all nations.

In conclusion, the Laser Patroller Satellite is a technology with immense potential for contributing to space governance and international cooperation on space debris mitigation. However, it is equally important to consider the potential implications of such advanced technologies for international relations and work together to ensure the responsible and sustainable use of space for the benefit of all nations.

Referințe

Al Amiri, S. 2023. "Governing space." *New Scientist* 257 (3423): 27. doi:https://doi.org/10.1016/S0262-4079(23)00157-4.

Association of Space Explorers. 2020. "Mitigation of Orbital Debris in the New Space Age." https://www.space-explorers.org/resources/Documents/Mitigation%20of%20Orbital%20Debris%20in%20the%20New%20Space%20Age-ASE%202020.pdf.

Botezatu, U.E. 2021. „Conflictele hibride și tehnologiile spațiale: implicații privind creșterea rezilienței societale." În *Managementul sustenabilității și sustenabilitatea managerială între paradigme clasice și moderne*, de D.E. Ranf, O.M.C. Bucovețchi și D. Badea, 234-245. Sibiu: Editura Academiei Forțelor Terestre „Nicolae Bălcescu".

Botezatu, U.E., and M.I. Piso. 2020. "Vital Outer Space Infrastructures: Romania's Pursuits and Achievements." În *Space Infrastructures: From Risk to Resilience Governance*, de U. Tatar, A.V. Gheorghe, F.K. Omer și J. Muylaert, 329 – 336. doi:10.3233/NICSP200033.

Budning, K., A. Wilner, and G. Cote. 2021. "A view from above: Space and the Canadian Armed Forces." *International Journal* 76 (4): 594–605. doi:https://doi.org/10.1177/00207020211067944.

Choi, S.H., and R.S. Pappa. 2020. "Assessment Study of Small Space Debris Removal by Laser Satellites." https://ntrs.nasa.gov/api/citations/20120009369/downloads/20120009369.pdf.

Dawson, L. 2017. "The politics and perils of space exploration: Who will compete, cooperate, dominate?" doi:https://doi.org/10.1007/978-3-319-38813-7.

European Space Agency. 2020. "The current state of space debris." https://www.esa.int/Space_Safety/Space_Debris/The_current_state_of_space_debris.

—. n.d. "Space debris by the numbers." Accesat 12 mai 2023. https://www.esa.int/Safety_Security/Space_Debris/Space_debris_by_the_numbers.

Finkleman, D. 2010. "Chapter 12 – Space situational awareness and space traffic management standardization." Vol. 144, în *Space Safety Regulations and Standards*, de Joseph N. Pelton și Ram S. Jakhu, 137-145. doi:https://doi.org/10.1016/B978-1-85617-752-8.10012-1.

Fix, A., G. Naletto, I. Hutchinson, N. Karafolas, W. Riede, A. Heliere, B. Menzies, and H. Riris. 2019. "Space Lidar and Space Optics." *CEAS Space Journal* 11: 359–362. doi:https://doi.org/10.1007/s12567-019-00288-2.

Gokon, H., S. Koshimura, J. Post, C. Geiß, E. Stein, and M. Matsuoka. 2014. "Detecting building damage caused by the 2011 Tohoku earthquake tsunami using TerraSAR-X data." *2014 IEEE Geoscience and Remote Sensing Symposium, Quebec City, QC, Canada.* 1851-1854. doi:doi: 10.1109/IGARSS.2014.6946816.

Hays, P.L. 2020. "International Space Security Setting: An Introduction." în *Handbook of Space Security*, de P.L. Hays. Springer, Cham. doi:https://doi.org/10.1007/978-3-030-22786-9_60-2.

Hebert, K.D. 2014. "Regulation of Space Weapons: Ensuring Stability and Continued Use of Outer Space." *Astropolitics* 1-26. doi:https://doi.org/10.1080/14777622.2014.890487.

Jakhu, R.S., and J. N. Pelton. 2021. "Global Space Governance: An International Study." doi:https://doi.org/10.1007/978-3-319-54364-2.

Johnson-Freese, J. S. 2007. "China's Space Ambitions." doi:https://doi.org/10.1080/10670564.2018.1497035.

—. 2021. "China's Race to Space: A Conversation with Joan Johnson-Freese." https://www.csis.org/podcasts/chinapower/chinas-race-space-conversation-joan-johnson-freese.

Klinkrad, H. 2023 . "Space debris: challenges and opportunities." https://www.mdpi.com/journal/aerospace/special_issues/Space_Debris_Removal_Challenges_Opportunities.

—. 2006. *Space debris: models and risk analysis.* Springer Science & Business Media.

Liou, J.C., N.L. Johnson, and N. Hill. 2014. "The NASA orbital debris engineering model ORDEM 3.0." *Proceedings of the 6th European Conference on Space Debris, 369-374.*

NASA. 2021. "NASA's efforts to mitigate the risks posed by Orbital Debris." https://oig.nasa.gov/docs/IG-21-011.pdf.

Oliveira Martins, B., K. Lidén, and M.G. Jumbert. 2022. "Border security and the digitalisation of sovereignty: insights from EU borderwork." *European Security* 31 (3: Digital/Sovereignty and European Security Integration): 475-494. doi:https://doi.org/10.1080/09662839.2022.2101884.

Papadimitriou, A., M. Adriaensen, N. Antoni, and C. Giannopapa. 2019. "Perspective on space and security policy, programmes and governance in Europe." *Acta Astronautica* 161: 183-191. doi:https://doi.org/10.1016/j.actaastro.2019.05.015.

Schall, W.O. 1991. "Orbital debris removal by laser radiation." *Acta Astronautica* 24: 343-351. doi:https://doi.org/10.1016/0094-5765(91)90184-7.

Scotti, V., M. Giannini, and F. Cioffi. 2020. "Enhanced flood mapping using synthetic aperture radar (SAR) images, hydraulic modelling, and social media: A case study of Hurricane Harvey (Houston, TX)." *Journal of Flood Risk Management* 13 (4): 18-62. doi:https://doi.org/10.1111/jfr3.12647.

Shen, S., X. Jin, and C. Hao. 2014. "Cleaning space debris with a space-based laser system." *Chinese Journal of Aeronautics* 27 (4): 805-811. doi:https://doi.org/10.1016/j.cja.2014.05.002.

Słomczyńska, I., and P. Frankowski. 2016. "Patrolling Power Europe: The Role of Satellite Observation in EU Border Management." În *EU Borders and Shifting Internal Security*, de R. Bossong și H. Carrapico. Cham: Springer. doi:https://doi.org/10.1007/978-3-319-17560-7_4.

Sormani, M.C., P. Bianco, and A. P. Rossi. 2016. "Space debris detection and monitoring using laser technology: present and future applications." *Journal of Sensors* 1-16.

SSPI Association. 2022. "How satellites make a better world." doi:https://doi.org/10.1016/j.spacepol.2013.02.004.

Stansbery, Gene. 2021. "NASA – Orbital Debris Program Office." https://www.nasa.gov/sites/default/files/files/OrbitalDebrisProgramOffice.pdf.

Syed, A.A., M. Mujahid, and M.Z.A. Syed. 2021. "Survey and technological analysis of laser and its defense applications." *Defence Technology* 17 (2): 583-592.

Valsecchi, G.B., and A. Rossi. 2002. "Analysis of the Space Debris Impacts Risk on the International Space Station." *Celestial Mechanics and Dynamical Astronomy* (Springer) 83: 63–76. doi:https://doi.org/10.1023/A:1020174528386.

Weeden, B.C., and V. Sampson. 2020. "The geopolitics of space security: Implications for Australia." *Australian Journal of International Affairs* 74 (1): 50-70.

Wei, Y., and C. Yang. 2021. "Space-based technologies for border security and management: A review." *Progress in Aerospace Sciences* 122: 101-154.

Wei, Y., Y. Zhang, and Y. He. 2021. "Space-based surveillance technologies and their maritime security applications." *Journal of Marine Science and Engineering* 9 (3): 307-311. doi:https://doi.org/10.3390/jmse9030307.

Wiser, L., and A. Timiebi. 2023. "An evolving space governance system: Balancing interests in five policy debates." *Acta Astronautica* 203: 537-543. doi:https://doi.org/10.1016/j.actaastro.2022.11.023.

Zhang, H., M. Long, H. Deng, S. Cheng, Z. Wu, Z. Zhang, A. Zhang, and J. Sun. 2021. "Developments of Space Debris Laser Ranging Technology Including the Applications of Picosecond Lasers. 2021; 11(21):10080." *Applied Sciences* 11 (21). doi:https://doi.org/10.3390/app112110080.

Zhang, Y., C. Wang, Y. Bai, and J. Guo. 2020. "Research on the Key Technology of Space-based Laser Debris Detection." *Journal of Aerospace Information Systems* 17 (3): 163-173.

Zhao, Q., L. Yu, Z. Du, D. Peng, P. Hao, Y. Zhang, and P. Gong. 2022. "An Overview of the Applications of Earth Observation Satellite Data: Impacts and Future Trends." *Remote Sensing* 14: 1863. doi:https://doi.org/10.3390/rs14081863.

Zhao, X., Y. Tang, S. Tan, and Q. Wu. 2017. "Design of laser communication system for space traffic management." *Acta Astron autica* 130: 10-17.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY
https://buletinul.unap.ro/index.php/en/

Development of european security and defence cooperation in support of the European Union's external action. Financial sustainability and institutional convergence

Dragoș ILINCA, Ph.D.*

*The Institute for Defence Political Studies and Military History
of the Ministry of National Defence, Bucharest, Romania
e-mail: dilinca@yahoo.com

Abstract

Optimizing the European Union's external action requires a comprehensive approach to linking relevant EU instruments and policies to the development of interaction and practical arrangements for cooperation with third countries. An extremely important component concerns the interaction between the Common Security and Defence Policy (CSDP) and external action, whose dynamics have undergone notable developments in recent years. The substantial progress made in the development of an integrated formula for promoting external action validates the central assumption of the present study that European cooperation in the field of defence tends to become one of the important supporting elements of external action. Starting from this assumption, another direction of in-depth analysis in the following pages concerns the ambivalent relationship between the financial support that external action receives through the new Multiannual Framework 2021-2027 and the concrete initiatives developed under the aegis of CSDP with military applicability.

Keywords:
CSDP; CFSP; EUGS; EPF; EDF; ENP; Multiannual Financial Framework; NDICI; IcSP; CBSD; APF; ATHENA Mechanism.

https://doi.org/10.53477/2284-9378-23-19

European cooperation in the field of security and defense represents one of the most dynamic projects developed in the context created by the adoption of the Treaty of Lisbon. The progress made in this field, both through capability projects and through the EU's numerous operational commitments in the field of crisis management, represents concrete arguments in this direction. Undoubtedly, European cooperation of this type has evolved over a period of time with a certain historical consistency. Basically, we are talking about a temporal perspective that covers almost half a century, whose initial moments are placed in the post-war context, and anchored in the debate that accompanied the restoration of Europe and the creation of European and Euro-Atlantic institutions.

The establishment of the European Union and the subsequent stages of progressive maturation of the security and defense dimension generated a complex institutional picture in which the security and defense aspects intersect with the expressions of external action, respectively with the instruments of financial assistance.

Chronologically, we can talk about a significant gap generated by the way in which the European institution developed. Practically, the external action and the development of the external assistance instruments can be identified from the initial stages of the operation of the European Economic Community, benefiting from fundamental structures after the adoption of the Maastricht Treaty and, subsequently, the establishment of the European Union. This period also corresponds to an approach focused on the security dimension, in the civilian sense of the term. The issue of European cooperation in the field of defense was confined to the institutional context provided by NATO and, sequentially, under the auspices of the Western European Union. After the adoption of the Treaty of Amsterdam (1997), cooperation in the field of defense under the auspices of the European Union acquired a much more concrete perspective in the direction of connecting it with other institutional dimensions of the EU.

The particularities generated by its intergovernmental character were reflected, however, with moderation regarding the structuring of an integrated matrix of this interaction. From this perspective, we can talk about maintaining, between 1997-2007, a relatively separate path between the evolution of external action and cooperation under the auspices of the European Security and Defense Policy (ESDP). The specific character of defense in the EU context contributed to maintaining this evolution, the connection of the mentioned domain to the external action instruments being carried out only sequentially and without being integrated into the financing system associated with the international profile of the EU. Obviously, the notable exception was represented by the civil component of the ESDP, whose parameters were fully integrated into the institutional and financial context of the EU, becoming a constitutive element of the external action.

The launching, in 2004, of the European Convention on the elaboration of a new EU Treaty also addressed the possibility of associating the defense dimension in support

of the EU's external action. Even if the product of the Convention, known as the Constitutional Treaty, failed in the ratification process carried out at the level of the member states during 2005, most aspects related to the development of cooperation in the field of defense were taken over at the level of the Treaty of Lisbon, adopted in 2007.

Starting from these developments, the present study aims to analyze how the context created by the new EU Treaty contributed to the rapprochement between cooperation under the aegis of the Common Security and Defense Policy (CSDP) and external action. In particular, the defense dimension is addressed and how it has become one of the important vectors for promoting the EU's external agenda, including through assistance in the field of crisis management. The implications of this approach are explored within the study and from the perspective of options for substantiating a new paradigm of financial and conceptual sustainability of external action. Within it, the issue of defense has become an integral part of the EU's tools for supporting a multidisciplinary and global external commitment. Thus, in addition to elements of a historical perspective, the study analyzes the practical evolutions of the cooperation and assistance instruments developed by the EU and the manner of their interaction with the defense dimension.

Institutional milestones in the implementation of the provisions of the Treaty of Lisbon

In addition to the major political importance that the adoption of the Treaty of Lisbon has for the development of the European Union, its particular significance concerns the field of security and defense. Taking over the conceptual philosophy and concrete benchmarks agreed by the member states in the context of the European Convention, the Treaty of Lisbon represented a particular impulse for the integrated development of this field in relation to other institutional and political dimensions of the European Union. The general tendency of the studies dedicated to analyzing the way in which the Treaty of Lisbon has influenced cooperation in the field of defense is to focus on the practical effects in the field of capabilities and crisis management operations that the EU will carry out at the global level. Obviously, this approach is validated by the extraordinary dynamics with which the issue of defense becomes a norm in the context of the European Union. However, the new breath brought by the Treaty exceeds this perimeter, with substance effects being identified at the level of the way of supporting the external action of the European Union. Thus, the EU Global Security Strategy (EUGS), adopted at the beginning of June 2016, brought to attention the importance of the connection between external action and the CSDP from the perspective of developing a Union capable of meeting the challenges of the security environment (European Union External Action 2016, 46). In this context, a number of objectives were placed that the EUGS was advancing in order to allow for the swiftest possible engagement of the instruments at its disposal

in support of external action. Through this approach, EUGS came to bring an additional emphasis to the provisions of the EU Security Strategy (2003), in particular on the fact that the development of European cooperation is an integral part of the external action promoted by the European Union in relation to different geographical perimeters. Along these lines, support to partner states through the CSDP would be the second pillar[1] of the level of ambition that the EU had assumed through the EUGS. In essence, it aimed at how European security and defence cooperation could support partner states' efforts to strengthen their resilience in synergy with other EU instruments and policies. The focus on the resilience dimension was from the perspective of the interaction between security and development, including the post-conflict stabilization and recovery effort. The main course of action was the contribution of the CSDP to the development of the potential of the partner states and the reform of the security and defence sector at their level.

[1] Together with *the Response to External Crises and Conflicts* and *the Protection of the Union and its citizens*.

The involvement of the CSDP instrumentation was intended to be carried out in complementarity with the policies and instruments that the EU benefited from in relation to the partner states. The modalities of effective engagement of EU support covered a wide range of possibilities, both in terms of assistance and expertise and in areas such as strategic communication, cybersecurity, and border security (Council of the European Union 2016, 12). From this perspective, the assistance provided to the partner states in the extended spectrum of the issues covered by resilience was to be carried out in close connection with the European Neighborhood Policy (ENP) having as geographical applicability the two dimensions – East and South. It should be noted that the adoption of the EUGS corresponded to an extremely important moment in the process of reviewing the implementation framework developed under the aegis of the ENP. The two geographical dimensions would be connected in order to ensure the coherence of the objectives aimed at stabilizing the EU's neighborhoods. In this respect, the security dimension was to represent an important component of the New European Neighborhood Policy, including an extensive set of areas of cooperation with regional valences such as security sector reform, fight against terrorism, prevention of radicalization, fight against organized crime, cyber protection, CBRN (European Commission 2015b, 14). However, the relevance of the ENP review process was largely conferred on the inclusion in the framework of the cooperation police with the states in the immediate vicinity of the issue of crisis management, subsumed by the dialogue on security and defence issues. The approach was structured from two perspectives and in a multidisciplinary vision corresponding to the complexity of the security environment but also to the potential for cooperation that the development of CSDP had registered up to that moment. Thus, the new ENP assumed cooperation with the partner states in the management of protracted conflicts, the concrete options envisaged including various topics such as

the exchange of good practices, the development of common objectives, and the strengthening of the internal capacity of the partner states. The security and defence dialogue was matched by the possibility of associating them with the activities and programs carried out by the EU structures responsible for managing the CSDP, as well as by supporting the participation of partner states in EU operations and missions. At the same time, it was envisaged to deepen the security dialogue in an extended paradigm and to the aspects related to the capacity of states in the field of early warning, prevention, and preparedness for crisis management and response (European Commission 2015a, 14).

Options for financing defence cooperation

Ensuring the financial resources needed to implement this ambitious agenda has become of particular importance. Most of the possibilities for financing the cooperation programs with the partner states can be found at the level of the European Neighbourhood Policy Instrument (ENI). Created in 2014, it provided a financial envelope of about 15.5 billion. Euro, for the period 2014-2020 (corresponding to the Multiannual Financial Cycle 2014-2020) from which a number of 16 partner states could benefit[2]. The funding possibilities offered by FTE concerned bilateral assistance, programs for several countries, and cross-border cooperation (European Union 2014a, 33). The area of applicability covered a wide range of areas associated with the development of regional cooperation in the two neighborhoods, institutional construction at the state level, resilience, economic development, potential for crisis, and conflict management.

[2] Algeria, Armenia, Azerbaijan, Belarus, Egypt, Georgia, Israel, Jordan, Lebanon, Libya, Republic of Moldova, Morocco, Palestinian Territories, Syria, Tunisia, Ukraine.

However, defence cooperation was not among the areas eligible for FTE funding (European Union 2009, art.41(2)). This was due to the EU regulatory framework according to which defence aspects could not be financed by funds from the EU budget. Thus, the whole set of instruments to financially support external action could not be used to finance defence cooperation activities. Security issues as well as the border issues between crisis management and post-conflict stabilization could use these possibilities in compliance with the civilian profile at the level of the implementation process. This is the case for the use of the Instrument for Stability and Peace (ICsP), created in 2014, which could financially support activities associated with crisis response, conflict prevention, peacebuilding, and crisis management preparedness (European Union 2014b, 3). Under the impact of the agenda put forward by the Global Strategy, the approach to military and defence issues in the context of external action would undergo significant transformations, also reflected in the way of structuring the instruments that the EU could use. Thus, since December 2017, IcSP has incorporated a new type of assistance

https://doi.org/10.53477/2284-9378-23-19

called Capacity Building in Support of Security and Development (CBSD). The main novelty that CBSD brought was the possibility of involving the military segment in the development of security and development programs (demining, civil protection tasks, reconstruction or rehabilitation of civilian infrastructure) that could not be met by civilian actors due to local security conditions (European Commission 2017b).

The logic of creating additional funding possibilities outside the EU budgetary framework through so-called off-budget instruments has also been used to develop ways to support the EU defence dimension. Launched between 1998 and 199, the latter has rapidly evolved towards a coherent formula for interaction, declined both through cooperation projects in the field of defence capabilities and through the launch in the following years of a significant number of crisis management missions and operations. If for civilian ones the financing could be done through the EU budget - The Common Foreign and Security Policy (CFSP) Chapter (European Union 2007, 41), this type of resources could not be used for military operations. Thus, on 23 February 2004, the Council of the EU adopted the decision establishing a mechanism for managing the common costs of military operations, known as the ATHENA Mechanism. The basis for this was found in the decisions of the Feira European Council (19-20 June 2000) which set out the general benchmarks for the functioning of the mechanism and, subsequently, its structuring on three levels: the minimum set of expenditure which may be subject to joint funding by all Member States regardless of whether or not it participates in the operation; the individual costs which were borne by the participating Member States; the possibility of extending the common costs by decision of the Council of the EU (European Parliament 2000). At the same time, the structure of common costs has been adapted to correspond to the main stages of carrying out military operational commitments (preparation-deployment in theatre-completion and withdrawal from the theater). Most of the military operations carried out between 2004 and 2020 benefited from the opportunities created through the ATHENA Mechanism that allowed the reduction of the effort for the contributing states with forces and capabilities. However, the share of common costs relative to the entire expenditure envelope associated with military operations was relatively modest, hovering around 10% (European Parliament 2021). The subsequent amendments to the operating decision (2011, 2015) also brought only marginal progress in increasing common costs.

A particular case in the evolution of financial mechanisms to support external action is the EU-Africa relationship. The main instrument of cooperation on this geographical coordinate was the European Development Fund (EDF), created in 1957 to finance cooperation programs with Pacific, Caribbean, and African states. Structured outside the Multiannual Financial Framework, EDF will ensure continuity of funding for these states only on the basis of member states' contributions, outside the budgetary envelope covered by the EU Treaty. The security and defence dimension become particularly visible within EDF and is associated with the

development of the EU's operational role in the field of crisis management in Africa. On these coordinates, a new cooperation instrument, known as the African Peace Facility (APF), was created on 19 April 2004.

Functionally, it has been framed in the institutional and financial context with significant autonomy determined by its specific nature. To a large extent, the profile of the FMA has been oriented towards the field of crisis management, helping to support the operational commitments made under the leadership of the. Over 3.6 billion Euro has been allocated to these areas, thus representing the European Union's contribution to the effort[3] of other crisis management organizations in this geographical area (UN, African Union). The structure of the APF assistance covered both the operational peace support component as well as separate assistance measures to support security sector reform in African states such as national capacity building and the Rapid Crisis Response Mechanism. The latter also had as a priority the development of the potential of the African Union to generate an adequate, timely, and adapted response in the security context of different regions of the African continent. It can thus be argued that the APF was an instrument of financial assistance that contributed significantly to supporting the operational effort carried out, in particular, by the African Union in the context of the successive crises carried out at various hot spots in Africa. The positive effects generated by the APF were particularly visible in terms of strengthening the EU's operational capacity, the contribution of this instrument being of particular importance in ensuring the sustainability of the operational commitments and, subsequently, the credibility of the stabilization and reconstruction effort. However, a number of geographical limitations are distinguished, with the functionality of the APF not corresponding to other geographical perimeters. This, combined with the relative impossibility of maximizing the effects of the ATHENA Mechanism in terms of common costs, has been considered with the utmost care in the context of the negotiations that preceded the adoption of the new Multiannual Financial Framework 2021-2027.

[3] Mention may be made of: the AU Mission in Somalia (AMISOM), Guinea Bissau (ECOWAS), the Lake Chad basin, the monitoring of the ceasefire agreement in southern Sudan, observation in Burundi, ECOWAS in the Gambia, G5 Sahel.

Clearly, the discussions on this topic have embedded a substantial component dedicated to making the EU's external action more effective on the coordinates advanced by the EU Global Strategy and shared by European Commission, by European Defence Action Plan. Last but not least, it should be noted that these debates overlapped with a process of accelerated maturation of the process of implementing the objectives of the new strategic framework visible both through the launch of new initiatives in the field of capabilities (Permanent Structured Cooperation – PESCO and through a consistent inventory of military (6) and civilian operations and missions (10) (European Union External Action 2019, 9). The upward trend in the development of the operational profile indicates the need for a more ambitious approach to the financial sustainability of the EU's capacity to generate operational

https://doi.org/10.53477/2284-9378-23-19

commitments. The overall profile of the EU's contribution in the area of security and defence also had to be reflected in the way it was externally acted on and, subsequently, in its financial support capacity. The question cannot be ruled out and the degree of interaction between external action and the manifestation of the CSDP, which was becoming an increasingly important component in supporting the EU's global role.

One of the direct consequences was found in the need for greater visibility of the defence issue at the level of external action, while at the same time increasing funding opportunities under the particular conditions offered by the EU Treaty. At that time, the interest in strengthening cooperation in the field of security and defense with partner states was not thoroughly addressed at the level of the assistance mechanisms. Even in the case of the APF, the core of external action was focused on supporting the role of international organizations in crisis management issues. The perspective promoted by the EUGS was much broader, reflected in its level of ambition for strengthening the link with partner states on the basis of cooperation programs of mutual interest (e.g. migration, energy security, terrorism, organized crime).

All these elements were in addition to the requirement to systematize successively generated financial support instruments in the context of the negotiations on the definition of the multiannual financial framework. It became extremely necessary to ensure correspondence of the existing instruments with the global priorities advanced by the EUGS, an objective which entailed, first of all, a much greater flexibility in terms of the functionality of these instruments, in particular as regards their geographical applicability. The systematization approach also implied the efficiency of the way of allocating and using the financial resources, simultaneously with the prioritization of the support for the states in the immediate vicinity of the European Union.

Multiannual Financial Framework 2021-2027. A new approach

As it can be seen, the landscape of the external action instruments was one of the most diversified in the institutional ensemble of the European Union. The assistance provided through the APF has been reinforced since 11 March 2014 through the Instrument for the Development of Cooperation (DCI) which operated in the 2014-2020 financial cycle. It will focus on the area of economic development and poverty reduction, including a distinct component in terms of cooperation with African states. Thus, DCI was in addition to the other five instruments for financial support of external action: the European Instrument for Democracy and Human Rights (EIDHR), the European Neighborhood Policy Instrument (FTE), the Instrument for Stability and Peace (IcSP-CBSD), the Partnership Instrument (IP) and the Instrument for Pre-Accession (IPA). The degree of fragmentation of the way in

which financial resources were capacity through these instruments is distinguished, at the level of which the harmonization of agendas was not the most consolidated.

This would be reflected, together with the above-mentioned approaches, in the framework of the new EU multiannual budget adopted in May 2018 covering the period 2021-2027. It had a number of peculiarities, including that it was the first multi-annual EU budget not to include Britain. In absolute values, BREXIT caused a decrease in the total budget (1.073mld. Euro compared to 1.082 billion in the previous perspective) situation compensated by an additional effort by Member States to increase contributions. At the same time, it was looming as a modern budget, focused on promoting investments in research, simultaneously with the capitalization of new technologies, but also of increasing the EU's contribution to environmental protection and reducing the impact of climate change.

Another major change was represented by the restructuring of the external action mechanisms, by integrating most of the instruments into a separate budget chapter (Heading 6 – Neighborhood and World). The envelope allocated to it was 110.60 Billion Euro, structured on two components – Pre-Accession Assistance (14.16 Billion Euro) and External Action (95.75 Billion Euro). The latter included four components: Humanitarian Assistance (11.57mld.), CFSP (2.68 bn.), External Territories and States (0.5 Billion), and the Instrument for International Cooperation, Development and Neighborhood (NDICI). The latter, also known as NDICI – Global Europe, was an integrative formula of previous instruments and dedicated to cooperation with third countries. The pillars of the new instrument were represented by: geographical programs (60.38 billion) of which about 20 billion were dedicated to the states in the EU's neighborhoods; thematic programs (6.35 billion) including conflict prevention and stability, rapid crisis response mechanism, conflict prevention, resilience building, including in the light of external action priorities (European Commission 2021b, 19).

Thus, the new financial perspective promoted a particular focus on the thematic dimension, which differed from the approaches used to structure previous budgets where external networking was viewed exclusively geographically. From this perspective, an additional possibility was created to strengthen the support provided to partner states (in the immediate vicinity) by adding, simultaneously, a surplus of cohesion and financial predictability of the external action carried out by the European Union. The influence of the level of ambition assumed by the Member States through the EUGS in terms of strengthening the EU profile as a relevant global player in the context of crisis management is also distinguished. NDICI was therefore capable of providing the financial ingredients to support that objective at a higher level. Compared to the allocations of the previous financial year, the significant increase in allocations for external action is distinguished, from 58.7 billion (Global Europe in 2014-2020) (European Commission 2014) at approximately EUR 80 billion, via NDICI (European Commission 2021b, 19). It represents an increase dictated by

https://doi.org/10.53477/2284-9378-23-19

the realities of a European Union that is much more actively engaged in the international context. At the level of this commitment, the general issue of crisis management, even if addressed *in extenso* by including military aspects, was an essential component.

We can talk about another feature of the new financial framework, namely the EU's contribution in the field of crisis management and the link with external action. With this, the EU's broader profile relies on coordinates of multi-disciplinarity, increasingly encompassing security aspects with extensive geographical applicability. The same approach was reflected in the resizing/restructuring of external action through the use of off-budget instruments. The new financial perspective sought to promote a pragmatic approach in using these opportunities, including from the perspective of supporting the military aspects of crisis management in relation to partner states. Undoubtedly, the main innovation was aimed at creating the European Peace Facility (EPF), an instrument dedicated to military matters under the auspices of PESCO. Structurally, this instrument came to fill the gap created by the impossibility of financing the military aspects. Responding to the general approach of systematization of financial instruments promoted in the development of the new financial framework, the EPF incorporated financing mechanisms for military operations (ATHENA) and assistance to Africa (EPF). This process was the main milestone of internal structuring of the new instrument that will be organized on the pillar model. Pillar I is thus dedicated to financing the common costs associated with EU military operations, taking over the functional typology of the previous mechanism. The second pillar is the main innovation to finance military and defence assistance measures. Thus, the EPF's regulatory framework stipulates that the assistance measures concern two types/areas that may be subject to funding through this particular instrument: actions to strengthen the capacity of third States and regional or international organisations in the military and defence fields; support for the financing of the military aspects of peace support operations led by regional, international organizations or by third states (European Union 2021a, 18).

Support to third countries could take the form of different formulas, including the provision of lethal and non-lethal equipment and materials. The budget associated with this initiative at the time of launch was approximately 5 billion Euro, for the period 2021-2027. So far, the beneficiaries of the assistance through the EPF have targeted the[4] states in the EU's neighborhoods as a matter of priority, thus corresponding to the overall profile of this instrument. The assistance measures also included the costs of the military components of African Union-led peace support operations previously financed through the African Peace Facility. In the context of the outbreak of the war in Ukraine, the EU's support for the Ukrainian armed forces has empowered the potential of the EPF, the level of assistance provided amounting to approximately 4 billion.

[4] The states whose armed forces have received financial support through Pillar II EPF are: Ukraine, Republic of Moldova, Georgia, Nigeria, Bosnia and Herzegovina, Mozambique, Mali, Lebanon, Mauritania.

Against this background, the European Council of 12 December 2022 endorsed the supplementing of the EPF budget by 5.5 billion Euro, of which 2 billion Euro were dedicated, according to the decision of the foreign and defence ministers of 20-21 March 2023, to the acquisition of ammunition.

Last but not least, it should be noted that the current Financial Framework is also a first in terms of including, for the first time, in the EU budget, costs related to the financing of initiatives in the field of defence cooperation between Member States. In this context, the European Defence Fund is placed, an initiative aimed at financing member states' cooperation projects in the field of capability development as well as on defence research. The budget of this initiative amounts to approximately EUR 8 billion for the period 2021-2027 (European Union 2021b, 162). Along with this, there is also the initiative to strengthen military mobility at EU level, which benefits from a 1.6 billion. Euro, for the same period (European Commission 2021a, 2).

Conclusions

Clearly, external action at European Union level is a dimension of utmost importance for supporting a global profile of this organization in the international security context. The progress made in recent years indicates a sustained trend towards strengthening this dimension, including from the perspective of better reporting the external action dimension to the realities and progress made in European security and defence cooperation. If for the period 2014-2020 it is possible to talk about a visible segmentation between the external action and the developments registered under the aegis of the CSDP, the new multiannual financial cycle has projected a new reality. The main feature of the latter concerns precisely the creation of an integrated matrix between the development of defence cooperation and external action. The role of the Global Security Strategy was, as in the case of other initiatives and projects developed in the CSDP context, a decisive one for the promoting deeply innovative measures.

The intrinsic value of the cooperation potential that the EU has begun to accumulate in terms of its defence and its practical declination in generating operational commitments are attractive elements at the level of cooperation with third countries. This conclusion is validated, both by increasing the complexity of the assistance and cooperation programs integrated into the overall profile of the EU's external action as well as the level of financial resources involved. Basically, the data presented in the study indicate a doubling of the resources allocated to supporting external action, under the conditions of a smaller multiannual financial perspective.

Under these auspices, the issue of defence has a particular significance, best illustrated by the potential that the various instruments of financial support for external action can have for designing a coherent and credible EU response in the contemporary security context. The role and contribution of the European Peace

Facility in recent times abundantly validate this assessment, the instrument being one of the main ways of supporting the EU's external action in support of Ukraine. Deepening the process of unlocking the potential that instruments such as the EPF and NDICI benefit from is a dimension on which the EU's attention will be focused in the coming period. The objectives assumed by the Member States in the framework of the Strategic Compass, adopted on 21 March 2022, aim precisely at this level, identified as one of the most important for strengthening the interaction between the developments in the CSDP and the EU's external action.

References

Council of the European Union. 2016. "Implementation Plan on Security and Defence." https://consilium.europa.eu/media/22460/eugs-implementation-plan-st14392en16.pdf.

European Commision. 2014. *Multiannual financial framework 2014-2020 and EU budget 2014 – The Figures.* doi:https://data.europa.eu/doi/10.2761/9592.

—. 2015a. "Review of the European Neighbourhood Policy." https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015JC0050.

—. 2015b. "Towards a new European Neighbourhood Policy." https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015SC0500.

—. 2017a. "Joint report to the European Parliament, the Council, the european economic and social committee and the committee of the regions – Report on the Implementation of the European Neighbourhood Policy Review." https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0018.

—. 2017b. "Stepping up support for security and sustainable development in partner countries." https://ec.europa.eu/commission/presscorner/detail/en/IP_17_5125.

—. 2021a. "Joint report to the European Parliament and the Council on the implementation of the Action Plan on Military Mobility from October 2020 to September 2021." https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021JC0026&from=EN.

—. 2021b. "The EU's 2021-2027 long-term Budget and NextGenerationEU." https://www.portugal2020.pt/wp-content/uploads/enn.en_.pdf.

European Parliament. 2000. "Santa Maria da Feira European Council 19-20 Junw 2000. Presidency Report on Strenghtening the European Security and Defence Policy." https://www.europarl.europa.eu/summits/fei1_en.htm.

—. 2021. "Report on the implementation of the Common Security and Defence Policy." https://www.europarl.europa.eu/doceo/document/A-9-2021-0358_EN.html.

European Union. 2004. "Council Decision 2004/197/CFSP of 23 February 2004 establishing a mechanism to administer the financing of the common costs of European Union operations having military or defence implications." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0197.

—. 2007. "Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union." *Official Journal of the European Union* C 326, 26.10.2012, 1-390. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF.

—. 2009. „Tratatul privind Uniunea Europeană (Versiune consolidată)." https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0001.02/DOC_1&format=PDF.

—. 2014a. "Regulation (EU) No 232/2014 of the European Parliament and of the Council of 11 March 2014 establishing a European Neighbourhood Instrument." *Official Journal of the European Union*, 15.03.2014, vol. 57, 27-44. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0232.

—. 2014b. "Regulation (EU) No 230/2014 of the European Parliament and of the Council of 11 March 2014 establishing an instrument contributing to stability and peace." *Official Journal of the European Union*, 15.03.2014, vol. 57, 1-11. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0230.

—. 2021a. "Council decision (CFSP) 2021/509 of 22 March 2021 establishing a European Peace Facility, and repealing Decision (CFSP) 2015/528." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0509.

—. 2021b. "Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092." *Official Journal of the European Union*, 12.05.2021, vol. 64, 149-177. https://eur-lex.europa.eu/eli/reg/2021/697/oj.

European Union External Action. 2016. *A Global Strategy for the European Union's Foreign And Security Policy – Shared Vision, Common Action: A Stronger Europe.* https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf.

—. 2019. "European Union Common Security and Defence Policy. Missions and Operations – Annual Report 2018." https://www.eeas.europa.eu/sites/default/files/20193237_ofab19001enn_pdf_0.pdf.

No.2/2023, APRIL-JUNE
https://doi.org/10.53477/2284-9378-23-20

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Hybrid – defining the concept of the 21st century warfare, operations and threats

Cpt. Georgiana-Daniela LUPULESCU, Ph.D. Candidate*

*Ministry of National Defence, Bucharest, Romania
e-mail: geo.lupulescu@yahoo.co.uk

Abstract

Hybrid threats, as well as hybrid war, have become our century's constant, receiving numerous definitions over time, which clarify to a greater or lesser extent these concepts characterized mainly by ambiguity both in terms of means, as well as the forces involved or the geographical area of combat. It can be deemed at least as derisive to try to define a concept that arose from the need to include everything that is known in terms of techniques, means, methods and tools, but also what will appear in the not-too-distant future, thanks to the rapid technological evolution, used by state actors and non-states in an attempt to achieve their most diverse goals, be they military, political, social or even economic. This paper aims to provide a brief overview of the relevant literature on hybrid threats, operations and warfare, starting from the first attempt to define them and up to new attributes added in the meantime. We will analyze the characteristics, types, actors involved, and objectives pursued by them, resulting from the combination of several techniques, methods or tools.

Keywords:
hybrid threats; hybrid warfare; psychological operations; cyber; terrorism; disinformation.

The end o Hybrid threats have become a constant of the 21st century, being present in most of the conflicts of recent years and manifesting at the same time in periods of apparent peace. The need to study and adapt both legislation and practice regarding the emergence of these new types of threats was first stated in the US National Defense Strategy in 2005 (Department of Defense 2005). The new challenges that the United States was facing at the time, which became even more apparent after the terrorist attacks of September 11, 2001, increased this need for defense rethinking and reorganization. As a result, military analysts have focused their efforts on theorizing, but also finding patterns to define, understand, and counter hybrid threats.

The present article aims, first of all, to clarify the concepts of hybrid threat, hybrid operation, hybrid conflict, hybrid campaign, and hybrid war, as well as to analyze the characteristics, types, actors involved and the objectives pursued by them, resulting from the combination of several techniques, methods or tools, generated by the in-depth study of the literature in the field, with the aim of increasing awareness and understanding of the concepts.

The concept of hybrid threat is very closely related to hybrid warfare, as they are tools used before, during and after the completion of the conflict. At the same time, some authors believe that the purpose of a hybrid threat is to exploit vulnerabilities without declaring war (Solik, Graf and Baar 2022).

At the same time, the concepts of hybrid operation, hybrid conflict or hybrid campaign differ not only from the perspective of unfolding over time but also from the awareness of the situation in which they are found by all the actors involved. In this sense, the hybrid operation may involve the use of a limited number of tools and for a shorter period of time, while, from a conceptual point of view, the hybrid campaign tends to be carried out for a longer time and involves a series of threats of hybrid type pursuing a well-defined goal. On the other hand, both concepts, both conflict and war, describe the situation in which the parties fail to resolve their differences amicably, using diplomatic instruments or with the support of the international community. The difference between the two concepts may also lie in their legal framework. Categorizing a conflict as a war grants certain rights to the warring parties and obliges them to comply with international regulations.

The concept of hybrid warfare was originally used to describe the actions of non-state actors and their ability to use both increasingly sophisticated military means and non-military instruments (Reichborn-Kjennerud and Cullen 2016), being later attributed to state actors as well, due to their use of hybrid threats. The US National Defense Strategy foresees the existence of four types of capabilities and methods: traditional, asymmetric, catastrophic and disruptive, as well as the fact that they overlap and that actors are expected to use two or more such methods simultaneously, as was the case in the wars in Iraq and Afghanistan where insurgents

represented both a traditional force and an asymmetric challenge (Department of Defense 2005). Frank Hoffman also argues that in the future it is expected that there will be separate combinations or hybrid threats targeting the United States' vulnerabilities and that actors will likely use all modes of combat, perhaps even simultaneously (Hoffman 2007).

Hybrid warfare began to be looked at with particular attention only after Israel's war in Lebanon against Hezbollah in 2006, when Israel faced a force of well-trained and equipped insurgents capable of conventional warfare but who acted using techniques and unconventional tools (Schnaufer 2017, 17-31). The war between Israel and Hezbollah was also addressed by Hoffman who considers it "the prototype of the modern hybrid war" (Hoffman 2007). In this first hybrid war, we, therefore, find the characteristics of this type of conflict, as it was predicted by the US National Defense Strategy (Department of Defense 2005) and defined for the first time by Hoffman (Hoffman 2007). The non-linear character of this type of war, as well as the involvement of non-state actors that combine the conventional way of fighting with capabilities from the asymmetric spectrum, are the defining elements of the war between Israel and Hezbollah.

With the annexation of Crimea by the Russian Federation in 2014, the phenomenon of "hybrid war" began to gain momentum, so it was no longer treated as a theoretical notion, but became a term used to describe the state of insecurity and challenges in the security address of Western states while continuing to be a topic of interest among theorists who focused their efforts, especially on hybrid threats from the Russian Federation. States have begun to include the concept in their own security policy, thus recognizing the importance and reality of the existence of hybrid threats and hybrid wars and creating the legislative framework for taking defensive measures against them. Some examples of this would be The National Military Strategy of the United States of America (2015), The National Defense Strategy of the country for the period 2015-2019 (2015), The National Defense Strategy of the country for the period 2020-2024 (2020), The National Strategy for Countering Hybrid Interference of the Czech Republic (2021), The National Security Strategy of the Republic of Poland (2020). Moreover, the 2015 United States National Military Strategy states that "such hybrid conflicts may consist of military forces assuming a non-state identity, as Russia did in Crimea, or may involve an extremist organization that has rudimentary combined arms capabilities, as demonstrated by the Islamic State in Iraq and Syria. Hybrid conflicts also may be comprised of state and non-state actors working together towards shared objectives, employing a wide range of weapons, as we have witnessed in eastern Ukraine" (Dempsey 2015) thus identifying and exemplifying the materialization of hybrid conflict characteristics.

The existence of hybrid threats and the need to counter them in a unified and effective way represent one of the main objectives of both Western states and NATO or the European Union. The latter defines threats and hybrid campaigns

as "multidimensional, combining coercive and subversive measures, using both conventional and unconventional tools and tactics (diplomatic, military, economic and technological) to destabilize the adversary. They are designed to be difficult to detect or attribute and can be used by both state and non-state actors" (European Commission 2018). Furthermore, at the NATO level, within the latest Strategic Concept, issued in 2022, reference is also made to the Alliance's support of its members and partners, as well as to the coordination of actions to combat hybrid threats with other relevant actors, such as the European Union (NATO 2022).

Threat, operation, conflict or hybrid war?

The alternative use of the terms threat, operation, conflict or war, to which is added the quality of hybridity, can create confusion, both among theorists and decision-makers. We believe that one of the causes of this fact is the ambiguous character of hybrid operations, as:

- there is no clearly delimited space for fighting, a war zone, but, especially due to the informational tools used, the conflict often exceeds state borders;
- the actors involved, whether they are state or non-state are not always known, such as the situation where a state actor sponsors a non-state actor acting in favor of the former;
- the existence of a very fine line between war and peace, that gray area, which Jan Almäng talks about extensively (Almäng 2019);
- targeting a state's vulnerabilities using hybrid tools and methods is a constant state of international geopolitics, with such actions not being categorized as acts of war. An example of this would be the Russian Federation's use of propaganda and disinformation (Veebel 2016, 14-19);
- the threat involves a hypothetical, potential situation, which is what distinguishes it mainly from any form of ongoing event.

Consequently, for the clarity of the terms, although sometimes they are categorized as hybrid conflicts and sometimes as hybrid wars, we will use the term hybrid war to name a declared conflict between two or more state or non-state actors, which use both conventional and unconventional means in order to achieve strategic objectives. Jan Almäng claims that "if a conflict qualifies as a war, the participants in the conflict acquire rights and duties that they did not have before" (Almäng 2019), which does not always serve the interests and objectives of the combatant forces, which is why the purpose of using hybrid threats and tools becomes even to generate a situation in which it is unclear whether or not a state of war exists, and if it does, who is and who is not a combatant (Thornton 2015, 40-48). Avoiding the use of the term war led to the more frequent use of other terms, such as: conflict, operation, action, campaign, etc. hybrids, all having more or less the same characteristics. The difference may lie in the scale of the action, if the combatant forces know each other, or if there are only attacks of any kind by an unknown actor, etc.

The threat to a state's security can be seen as a combination of capability, intent and opportunity. The hybrid character in this situation results from the type of tools used. If, for example, an actor has the technical and intellectual capacity to conduct a cyber-attack, has the intention to do so, most likely due to the need to achieve certain strategic objectives, and the opportunity to execute the attack also arises, most often generated by the identification of a vulnerability, then the possibility of that actor executing a cyber-attack becomes a threat to those who have vulnerabilities in that domain and are in that actor's area of interest. To illustrate, we recall the cyber-attacks led by the Russian Federation on Georgia in 2008, which began a few months before the outbreak of the conflict later considered "the first war to take place in air, sea, land and cyberspace" (Mihai 2022). In the mentioned example, we identify the ability of the Russian Federation to use hackers to carry out cyber-attacks (they were attributed to the Russian Federation only in 2020 (Roguski 2020), the intention, demonstrated by the coordination of cyber-attacks with the use of conventional forces and the political situation in Georgia at the time, which did not serve the interests of the Russian Federation ("The newly elected president, Mikheil Saakashvili, engaged in close proximity to Western structures and attempted to reintegrate the provinces of South Ossetia and Abkhazia." (Mihai 2022), and last but not least, the opportunity generated by the vulnerability of Georgian IT systems.

Probably one of the most common questions among researchers and decision-makers in the last decade was "What is hybrid war?". Numerous scientific works have addressed this theme in an attempt to define and state a series of specific characteristics of this type of conflict. Among the first to stand out and make an essential contribution is Frank Hoffman, he is the one who named the conflicts characterized by the simultaneous use of tools from several fields: military, IT, psychological, economic, and political, by well-trained and flexible forces. In his view, hybrid warfare involves a number of different ways of waging a war that includes conventional capabilities, but also techniques and tools specific to asymmetric warfare, terrorist acts, indiscriminate violence, coercion, and even criminal actions (Hoffman 2007). At the same time, Thornton claims that one of the main characteristics of hybrid warfare is that "modes of conflict overlap and merge. Thus, the battlespace, as it is, can be shaped at one level by conventional operations and irregular activities and concurrently, at a higher level, by the application of underlying political and economic pressures" (Thornton 2015, 40-48). We can thus deduce that hybrid warfare involves the combined use of conventional means, military forces, and instruments, with asymmetric means. On the other hand, from the definition of hybrid war, given by Giannopoulos, Smith and Theocharidou (2021, 11), namely "the deliberate combination and synchronization of actions, by a hostile actor, specifically targeting systemic vulnerabilities in democratic societies", we can extract one of the specific characteristics of hybrid warfare, the targeting of vulnerabilities. So, we are no longer just talking about attacks directed at opposing military forces, but also about identifying and exploiting the adversary's vulnerabilities, including the civilian, non-combatant population. Also, the types

of actions used, and the threats launched against the enemy forces or the civilian population are very varied, from ballistic missile attacks, to psychological operations or cyber-attacks, usually used simultaneously on various targets, to achieve strategic objectives. At the same time, hybrid war has a strong ambiguous character, both in terms of understanding and using the concept itself (Janičatova and Mlejnková 2021), hence the many definitions, more or less overlapping, as well as the creation of policies and taking concrete actions to prevent or combat hybrid risks or threats.

Another big question mark about hybrid warfare and threats is whether they are new or just another way of naming what was already known. There are voices that say hybrid wars are as old as war itself (Galeotti 2016, 282-301), but also that while they are not new, they are different (Hoffman 2009b). At the same time, Giannopoulos et. al. (2021) consider that the evolution of war towards this hybrid form is mainly given by the dynamics of the security environment, by new tools, concepts and technologies, used simultaneously to exploit vulnerabilities. Hybrid warfare is therefore a relatively new concept, but one that encompasses the novelty generated by technology and its use for hostile purposes. At the same time, although the concept was introduced and developed more than fifteen years ago with the issuance of the US National Defense Strategy in 2005, when they first identified the need to adapt legislation, policies and defensive measures against these types of threats, only after the invasion of Crimea in 2014 did the concept of "hybrid war" gain special importance among theorists and decision-makers. Thus, both NATO and the European Union started including the term "hybrid" in their own policies and strategies (Mikac 2022).

Another characteristic that we consider defining in terms of categorizing the conflict as a hybrid one is represented by the blurring of the states' borders and the lack of clarity in determining the period of the conflict. What we intend to highlight is the fact that the tools used in a hybrid conflict, whether we are talking about cyber-attacks, propaganda, disinformation or terrorist attacks, do not necessarily surface in times of conflict, in the framework of a declared war, but can constitute hybrid threats to the security of states, which furthers the discussion of whether it is really a hybrid war or just a natural competition between states (Wither 2016, 73-87).

Types of Hybrid Threats

Giannopoulos et al. (2021) developed a conceptual model of hybrid threats in terms of actors, tools, affected domains, activity and target, where the latter was established as undermining decision-making capability. The tools used are not necessarily illegal or hybrid actions. For example, from the extensive list of hybrid threats, provided by Giannopoulos et. al. (2021), military exercises or the support of some political actors are neither illegal activities, nor do they constitute stand-alone hybrid threats. Instead, certain combinations of such instruments, used simultaneously and aimed

at destabilizing society from a political, economic, social or military point of view, are part of the category of hybrid threats.

As with other issues related to wars and hybrid threats, when it comes to identifying the types of hybrid threats, the situation is far from clear. The hybrid character is given by a number of factors, if only one person shares a piece of fake news on a social network, we cannot speak of the existence of a hybrid threat. One always takes into account the actors involved, the combination of kinetic and non-kinetic means, the purpose of the threat, the strategic interests and objectives, and of course the presence of ambiguity in all the mentioned aspects, to be able to say that a war or a hybrid operation is taking place.

The rapid evolution of technology has led to the emergence of innovative types of threats that have long gone beyond the strictly military sphere. Although some of them have existed for a very long time, such as psychological operations, of which we mention propaganda and disinformation, the way in which they are used, the extent to which they are carried out and the characteristic subtlety pose great problems in identifying, preventing and combating these hybrid threats. Treyger et al. (2022) for example, points out that the information war waged by the Russian Federation threatens to erode belief in factual truths and cause concrete damage through disinformation.

At the same time, cyber-attacks occupy a place of honor in the types of tools used in a hybrid war, sometimes even being the main "fighting" tool. For example, Russia is known to use such tactics through state-funded hacker groups and examples are multiple, from the cyber-attacks against Estonia in 2007, to those against Georgia in 2008 or those against Ukraine, both in 2014 with the annexation of Crimea (Mihai 2022) as well as those associated with the current conflict (Smith 2022).

State and non-state actors using hybrid threats

When we talk about hybrid war or hybrid threats, an important part of the discussion is to focus on the types of actors involved, the connections between them and the specific characteristics of each one. First of all, actors fall into two broad categories: state actors and non-state actors.

Whether we are talking about state actors or non-state actors, the discussion cannot be in terms of black and white, since, as in the case of the types of actions used, borders, objectives, the line of demarcation between the two categories it is blurred, unclear. If we take as an example the Israeli war in Lebanon, mentioned earlier in the article, the fusion between a non-state actor – Hezbollah and a state actor – Lebanon is at least obvious. As Hoffman suggests, "Hezbollah [...] has demonstrated a range of military capabilities similar to those used by states, including thousands of short-

and medium-range rockets and projectiles. This case demonstrates the ability of non-state actors to study and deconstruct the vulnerabilities of Western-style armies" (Hoffman 2007, 35-36). At the same time, Hezbollah benefited from weapons and training from Lebanon, a fact that unequivocally demonstrates the fusion of non-state - state actor.

On the other hand, Janne Jokinen and Magnus Normark believe that the use of non-state actors by states has always occurred, but the power of non-state actors has increased with the development of technology and financial services, areas in which certain non-state actors became experts over time. Consequently, the likelihood of their being used by states has increased considerably. At the same time, non-state actors can also find themselves in the position of adversaries of states (Jokinen and Normark 2022).

Another aspect to be considered is the fact that regardless of the form in which a non-state actor presents itself, whether we are talking about individuals, more or less legally constituted organizations, armed groups, etc., there are still no international laws that state the regime, role or responsibilities of non-state actors in an unequivocal manner (Kleckowska 2020). So, both states and non-state actors take advantage of this situation, the former by using non-state actors to achieve their goals, sometimes in dubious circumstances, and the non-states by having on the one hand the freedom to collaborate or not with the states and, on the other hand, by being able to exert influence on the policies of the states.

Vladimir Rauta suggests a classification of non-state actors that constitute combat groups, taking into account the relationship between them and states, into proxy, auxiliary, surrogate and affiliated forces thus:

- proxy forces are armed groups; they are not part of the regular forces but fight for them or on their behalf;
- auxiliaries are not part of the regular forces, but collaborate with them, being incorporated into the structure of the forces;
- the surrogates are used by the regular forces to complement their forces or even to replace them completely;
- affiliates are those that fight for regular forces, remaining officially out of the conflict (Rauta 2019).

Such a classification results from the way states use non-state actors, their involvement and the manner in which it takes place. Certain things in reality are not so clear since hybrid warfare and the actors using hybrid threats are characterized by ambiguity and the involvement of non-state actors is not always visible, which makes it difficult, if not impossible, to identify and catalog all the actors involved.

Non-state actors can either support the state for various reasons, have common goals, share the same ideology, etc., or it is the states that support, as sponsors, certain

groups or organizations for the same reasons, in which case the official combatant is the non-state actor and the state is not officially involved in the conflict. Non-state actors can take the form of any combination of insurgent or terrorist networks, organized crime groups, social groups such as clans, tribes, or ethnic groups, or ideologically or religiously motivated organizations, all of which may or may not be overtly or covertly supported by to legitimate states or businesses (Giannopoulos, Smith and Theocharidou 2021). The large number of types of non-state actors, their capabilities that sometimes reach or even exceed those of the state do not make the work of those fighting against hybrid threats any easier.

Regarding the actors involved in hybrid operations, the biggest challenge in trying to prevent or counter a hybrid threat is primarily their identification (Jokinen and Normark 2022), as there are situations where one cannot establish with accuracy the involvement of a particular actor. States can benefit from this situation, in the sense that they can always deny and refute any accusation of involvement in hybrid activities and, according to Giannopoulos et. al. "states directing activities through non-state entities exploit the opportunity to carry out activities of a harmful nature against other countries covertly. This has the advantage of making it more difficult for targeted states to detect activity related to the harmful state and respond before it occurs, but also to hinder the ability of the targeted state to attribute the harmful operation to the foreign state behind the event or series of events" (Giannopoulos, Smith and Theocharidou 2021).

Goals, objectives and targets

Like any conflict that has taken or will take place, hybrid wars are also based on a goal, a motivation, some objectives. Most of the time they fall into the political sphere by influencing the policies of some states, decreasing the trust of the population in state institutions, in a word weakening the government of a state or even its collapse. At the same time, any vulnerability of the state can be exploited within a hybrid operation, this being the mode of action of hybrid threats, identifying and exploiting the vulnerabilities of a state or of the way of fighting (Hoffman 2007).

Before launching a hybrid operation, after establishing the objectives pursued, the next step is the target selection. This action is closely related to the identification of vulnerabilities to be exploited. According to Cederberg and Eronen, they include all military capabilities, internal security, the internal and external political area, the economy, infrastructure, the standard of living and the resilience of the population to psychological operations (Cederberg and Eronen 2015). The hybrid operation takes place at the intersection of the identified vulnerability, the attacker's ability to exploit this vulnerability and the objectives pursued by the latter. Cederberg and Eronen argue that "hybrid operations are based on using identified asymmetries to make operations successful by confronting one's own strengths against the known

weaknesses of targets" (Cederberg and Eronen 2015). In his article, Cîrdei also claims that the mode of action in hybrid operations is based on exploiting vulnerabilities but also avoiding direct confrontation (Cîrdei 2016, 113-119). At the same time, recent history proves to us that certain objectives still cannot be achieved without an active military component as is the case in the current Russian-Ukrainian conflict, which includes everything from armed aggression to cyber-attacks (Viasat 2022) or psychological operations (EU vs DiSiNFO 2022).

A particular reason why states would engage in hybrid actions, especially through non-state actors with certain capabilities, could be to gain access to certain infrastructures or systems. Such a situation is presented by Giannopoulos et. al. This is Airiston Helmi, a real estate company in Finland that could have been used as a cover to make important strategic investments and prepare the properties for later use. In this situation, Russian citizens would have bought very well secured properties, with exceptional technical equipment to accommodate a large number of people and located in an important strategic area of Finland. The author considers this a very good example of "how foreign states can act through third parties to influence, intervene or obstruct the affairs of states to generate negative consequences or to establish the ability to do so when desired" (Giannopoulos, Smith and Theocharidou 2021).

Conclusions

The hybrid attribute added to threats to the security of states and the wars waged in recent years has created polemics and differences of opinion both in the academic world and at political level. Hybrid wars and their complexity have been and will probably be studied for a long time to come especially because the information dimension, which often underlies the manifestation of many other types of threats, is in continuous development.

Although at the level of theorists there is no consensus regarding the use of the terms threat, conflict, operation or hybrid war, we can state that the tools used and the ways of combining them, the involvement of both non-state and state actors, the goals pursued and, perhaps most importantly, the ambiguity of all the above-mentioned aspects, are defining elements and actually the mark of the hybrid character of any threat, operation, any conflict or war.

The emergence and evolution of the concepts of threats and hybrid wars are not new. The hybridity of conflicts and threats does not create an entirely new concept, but one in a dynamic continuum, adapted to the technological capabilities of our times. Although the term "hybrid" entered the vocabulary of academics and political-military decision-makers almost 20 years ago, but more significantly after 2014, this way of fighting can also be observed in much older conflicts, especially when

we refer to the use of non-military tools such as propaganda or disinformation. Moreover, the hybrid character attributed to contemporary threats and conflicts began to be increasingly associated with their cyber dimension. The latter is a tool in itself but also a means of implementing other types of threats, which generates not only ambiguity but also the blurring of state borders, actions often taking place in cyberspace. Security and defense against hybrid warfare and threats have been and will continue to be a challenge, especially due to the inherent ambiguity, both in terms of the tools used, their combination and synchronization, and in terms of identifying the actors involved.

The evolution and dynamic character of the concepts of hybrid warfare and hybrid threat represent a challenge for the security of Western states. Their defining characteristics no longer allow either individual defense or treating each threat separately, but a joint approach of states, rigorous defense planning including all key areas of society will be required. Furthermore, identifying and mitigating society's vulnerabilities before they are exploited by hostile entities should be one of the main goals of states.

References

Administrația Prezidențială. 2015. "Strategia Națională de Apărare a Țării pentru perioada 2015-2019." https://www.presidency.ro/files/userfiles/Strategia_Nationala_de_Aparare_a_Tarii_1.pdf.

—. 2020. „Strategia Națională de Apărare a Țării pentru perioada 2020-2024."

Almäng, Jan. 2019. "War, vagueness and hybrid war." *Defence Studies* 19 (2): 189-204.

Cederberg, Aapo și Pasi Eronen. 2015. "How can Societies be Defended against Hybrid Threats." *Geneva Centre for Security Policy* (9).

Cîrdei, Ionuț Alin. 2016. "Countering the hybrid threats." *Revista Academiei Forțelor Terestre* (2): 113-119.

Dempsey, Martin. 2015. "The National Military Strategy of the United States of America." https://history.defense.gov/Historical-Sources/National-Military-Strategy/.

Department of Defense. 2005. "National Defense Strategy of the United States." https://history.defense.gov/Portals/70/Documents/nds/2005_NDS.pdf?ver=tFA4Qqo94ZB0x_S6uL0QEg%3d%3d.

EU vs DiSiNFO. 2022. "Key Narratives in Pro-Kremlin Disinformation: «Nazis»." https://euvsdisinfo.eu/key-narratives-in-pro-kremlin-disinformation-nazis/#.

European Commission. 2018. „Comunicare comună către Parlamentul European, Consiliul European și Consiliu." https://data.consilium.europa.eu/doc/document/ST-10242-2018-INIT/ro/pdf.

Galeotti, Mark. 2016. "Hybrid, ambiguous, and non-linear? How new is Russia's new way of war?" *Small Wars & Insurgencies* 27 (2): 282-301.

Giannopoulos, Georgios, Hanna Smith și Marianthi Theocharidou. 2021. *The lanscape of hybrid threats: A conceptual model.* Luxembourg: Publications Office of the European Union.

Hoffman, Frank. 2007. *Conflict in the 21st century: The Rise of Hybrid Wars.* Arlington, Virginia: Potomac Institute for Policy Studies.

—. 2009a. "Further Thoughts on Hybrid Threats." *Small Wars Journal.*

—. 2009b. "Hybrid Warfare and Challenges." *JFQ* (52): 34-48.

Janičatova, Silvie și Petra Mlejnková. 2021. "The ambiguity of hybrid warfare: A qualitative content analysis of the United Kingdom's political–military discourse on Russia's hostile activities." *Contemporary Security Policy.*

Jokinen, Janne și Magnus Normark. 2022. "Hybrid threats from non-state actors: A taxonomy." *Hybrid CoE Research Report.*

Kleckowska, Agata. 2020. "States vs. non-state actors – a public international law perspective." *Hybrid CoE Strategic Analysis.*

Mihai, Paul. 2022. „Provocări hibride de natură cibernetică." *Infosfera* (2).

Mikac, Robert. 2022. "Determination and Development of Definitions and Concepts of Hybrid Threats and Hybrid Wars: Comparison of Solutions at the Level of the European Union, NATO and Croatia." *Politics in Central Europe* 18 (3): 355-374.

Ministry of Defense Czech Republic. 2021. "The National Strategy for Countering Hybrid Interference of Czech Republic." https://www.army.cz/assets/en/ministry-of-defence/basic-documents/national-strategy---aj-final.pdf.

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

President of the Council of Ministers. 2020. "The National Security Strategy of the Republic of Poland." https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf.

Rauta, Vladimir. 2019. "Towards a typology of non-state actors in „Hybrid Warfare": Proxy, auxiliary, surrogate and affiliated forces." *Cambridge Review of International Affairs.*

Reichborn-Kjennerud, Erik și Patrick Cullen. 2016. "What is Hybrid Warfare?" *Policy Brief* (Norwegian Institute of International Affairs) (1).

Roguski, Przemyslaw. 2020. "Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace." https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/.

Schnaufer, Tad A. 2017. "Redefining Hybrid Warfare: Russia's Non-linear War against the West." *Journal of Strategic Security* 10 (1): 17-31.

Smith, Brad. 2022. "Defending Ukraine: Early Lessons from the Cyber War." https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

Solik, Martin, Jan Graf și Vladimir Baar. 2022. "Hybrid Threats in the Western Balkans: A Case Study of Bosnia and Herzegovina." *Romanian Journal of European Affairs* 22 (1).

Tenenbaum, Elie. 2015. "Hybrid Warfare in the Strategic Spectrum an Historical Assessment." In *NATO's response to hybrid threats*, by Guillaume Lasconjarias and Jeffrey A. Larsen, 95-112. Rome: NDC Forum Paper.

Thornton, Rod. 2015. "The Changing Nature of Modern Warfare." *The RUSI Journal* 160 (4): 40-48.

Treyger, Elina, Joe Cheravitch și Raphael S. Cohen. 2022. *Russian disinformation efforts on social media.* Santa Monica: RAND Corporation.

Veebel, Viljar. 2016. "Estonia confronts propaganda: Russia manipulates media in pursuit of psychological warfare." *Per Concordiam* 7 (1): 14-19.

Viasat. 2022. "KA-SAT Network cyber attack overview." https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.

Wither, James K. 2016. "Making Sense of Hybrid Warfare." *Connections: The Quarterly Journal* 15 (2): 73-87.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY
https://buletinul.unap.ro/index.php/en/

Researching disinformation using artificial intelligence techniques: challenges

Ștefan Emil REPEDE, Ph.D. Candidate*

*"Lucian Blaga" University, Sibiu, Romania
e-mail: stefan.repede@ulbsibiu.ro

Abstract

The present article aims to address a series of problems generated by the use of artificial intelligence models for the study of the creation and dissemination of false information beginning from the difficulties in defining and classifying established terms, continuing by exemplifying the way some of the established databases in the research field of fake news are built and ending by noting the differences in their labeling.

Keywords:
fake news; misinformation; disinformation management; natural language processing; NLP; artificial intelligence; machine learning; cyber security.

1. Introduction

Social media was initially seen as an expression of free speech, positive mobilization, and democracy. Currently, studies that include social networks rather categorize these as a threat to democracy (Yerlikaya and Aslan 2020). Social media platforms can be heavily used to manipulate the masses by various types of actors with political, social, monetary, or radical agendas. The issue of media influence on certain agendas emerged mainly after the event known as the Arab Spring and continued in the 2016 US political election, the UK Brexit, the 2017 French Presidential Election, the 2019 Turkish Election, the Pandemic of COVID-19 in 2019, all the way to the major escalation of the Russian-Ukrainian war in 2022. These events have been affected by propaganda campaigns and the spread of disinformation and fake news. The extensive use of disinformation worldwide has emphasized the need to create methods that can flag and combat the use of disinformation.

With the development of emerging technologies such as artificial intelligence (AI), the scientific community proposed various methods involving the use of technologies considered "state-of-the-art" with the aim to combat the phenomenon of creating and disseminating false information. An example of technology studied for the classification of written information from online media, the so-called fake news, was based on the use of Natural Language Processing (NLP) models. The discipline of natural language processing, also known as computational linguistics, is a branch of computer science that uses AI to research written and spoken human languages.

Misinformation and disinformation are classified as the 9th point of interest in the EU Cyber Security Agency's report of October 2022 (ENISA 2022), which states that the use of cloud computing resources, tools, and AI algorithms supports the fabrication of malicious information. The report also states that detecting and minimizing the spread of false information on social media is still among the most important technical approaches to disinformation management. This concept refers to the process of identifying, analyzing, and mitigating the spread of false or misleading information in order to minimize its negative impact on individuals, organizations, and society as a whole. Disinformation management involves steps such as monitoring the target media, detecting potential false information, comparing it with reality (fact-checking), cataloging it and establishing a response or the necessary countermeasures to counter it.

The first step in disinformation management is monitoring and detection (Schia and Gjesvik, 2020). This involves monitoring the spread of information across various platforms and channels such as social media, news websites, and online forums. Automated tools and manual analysis are used to identify potential disinformation campaigns and track their spread. After the detection phase, the next step is fact-checking, which involves checking the accuracy of the information presented.

This step is necessary to determine the appropriate response and countermeasures that should be taken (N. N. Schia 2020). Response and countermeasures involve developing and implementing strategies to counter the spread of the identified campaign or minimize its impact. The measures may include targeted advertising, public messaging campaigns, or requesting the flagging or removal of malicious information from various online platforms (Schia and Gjesvik, 2020).
Managing disinformation is a continuous process that requires collaboration between various stakeholders, including government agencies, media organizations, and civil society groups. Tackling disinformation in general requires a range of skills and expertise from those involved, expertise that includes data analysis, social media monitoring, communications, and public relations strategies. Overall, effective management of misinformation is essential in today's digital age, where the spread of false or misleading information can have serious consequences for individuals, organizations, and society as a whole (US Department of State 2023).

Unfortunately, according to the Global Risks Report 2023 (WEF 2023), disinformation management is a process that is either not initiated or is in its early development stage and its effectiveness is viewed as poor or extremely poor.
Disinformation management is a cybersecurity issue primarily because the spread of false information can be used as a tool to manipulate public opinion or create a false sense of reality (US Department of State 2023).

Fake news – possible definitions and categorizations

An initial problem that arose with the scientific study of the issue related to the creation, dissemination, and consumption of fake news was the definition of the concept. In principle, there are several criteria for the classification of false information, groupings in which the term fake news is only one of the proposed ways of manifestation (Zafarani, Zhou, et al., 2019). The problem imposed by the meaning of the term fake news has been widely discussed in recent years, especially against the background of several campaigns reported in the international media (Baptista and Gradim 2022). The term „fake news" is currently considered inaccurate from a technical point of view, because it describes a wide variety of mass media products, although it is (Gelfert 2018) currently present in the Romanian legislation in article 404 of the Criminal Code (Romanian Parliament 2009), which criminalizes „the communication or dissemination, by any means, of fake news, data or false information or falsified documents, knowing their false nature, if this endangers national security", the article is largely copied from article 168^1 of the version of the Criminal Code of Romania that dates from 1968 (Romanian Parliament 1968).

Speech or news that incites violence is easier to identify than speech that incites hatred, denigrates the rule of law, or slanders certain social groups. The latter is not always clearly identifiable. What is considered unacceptable to one individual may

https://doi.org/10.53477/2284-9378-23-21

be something completely different to another. This kind of difference of opinion creates a certain ambiguity about what constitutes hate speech in a digital context because this medium can include, in addition to outright falsehoods, mistakes in the reporting of facts, opinionated commentary, political satire, or inaccuracies. To disambiguate this often-referred-to concept, several types of classification of false/misleading information have been proposed, which are addressed in the following lines:

2.1. Classification by intent. A proposed classification of fake information, which includes the term fake news, was proposed in the Journal of the NATO Center of Excellence for Strategic Communications (NATO Strategic Communications Centre of Excellence 2020). Understanding the intent behind the campaign/fake news allows for addressing the causes of misinformation and developing prevention, education, or accountability measures. The classification contains several four categories that take into account the intention behind their propagation:

Disinformation – defined as the intentional creation and distribution of false/manipulated information with the intent to deceive/mislead. An example of disinformation can be considered back in 2022 when a false narrative was launched according to which the majority of Romanians want their country to leave NATO and the EU and there is no Romanian political party that can capitalize on this move. It was promoted by a local radio station linked in other situations to promoting misinformation and fake news. The narrative is contradicted by opinion polls (Necşuţu 2022a).

Misinformation – is that false/misleading information that has been distributed without the intention to manipulate or mislead. The main point different from the first type of misinformation representing it is the intention behind its spread. An example of mistaken news coverage occurred on 26 February 2022, when the television channel "Antena 3" mistakenly presented footage from a 2013 video game called Arma 3 as being from Russia's war against Ukraine (Radu 2022).

MALinformation – is a term created by media researcher Hossein Derakhshan, published as a co-author in a Council of Europe report entitled „Information Disorder" (Wardle and Derakhshan 2017) and later adopted by UNESCO. This refers to information that is true and contains correct references, but which is intentionally transmitted negatively to cause actual harm or the imminent threat of actual harm to a person, organization, or country. For example, a post made in the archive titled „Paradise Papers" (Osborne 2017) about the offshore investments of the British Monarchy revealed that many members of the royal family had evasive offshore investments. The campaign was intended to harm the British Monarchy and not to inform the public about their illicit practices.

Propaganda – information, predominantly biased or misleading, that is disseminated with the aim of promoting a cause or political point of view. An example of such a

narrative can be seen in 2022, when the war between Russia and Ukraine is depicted as a war waged by NATO against Moscow (Cezar 2022). The claim about an alleged NATO threat against Russia had circulated long before it was picked up in Romania. It was promoted by Russian propaganda to justify Moscow's appetite for new territories (invasion of Georgia in 2008, invasion of Ukraine in 2014 and 2022) and was based on older Soviet narratives that NATO „encircled" the USSR with its bases. As Russian forces began to claim defeat in Ukraine, the narrative was altered and the new claim is that Russia is actually fighting NATO/the West and that Ukrainians are being used as cannon fodder (Necşuţu 2022b).

Fake news – is information whose falsity is verified and which is intentionally spread. An example of fake news repeatedly circulated in Romanian media claims the Netherlands opposes Romania's accession to the Schengen zone because the maritime port of Constanța threatens the supremacy of the port of Rotterdam. This false narrative was reiterated in 2022 in the context in which Bucharest hoped that Romania would be admitted to the Schengen area by the end of the year (Peiu 2022). This type of news had already appeared 10 years earlier, originally released by the Voice of Russia. The fake news cycle states that the Netherlands will never agree to Romania joining the Schengen area, fearing that the port of Constanța could become the largest port in Europe, thus having an irreversible impact on the Dutch economy which relies heavily on the trade entering and leaving the port of Rotterdam. In fact, the competition between the two ports is out of the question, as the port of Rotterdam is better positioned geographically and has superior infrastructure and operational capabilities (Veridica 2022a).

2.2. Stylistic classification. Another approach to the classification of fake information, which includes the concepts of fake news, disinformation, and propaganda, is focusing on the stylistic way of composing media materials and includes a total number of 5 categories. It was proposed within the American State Library of North Dakota (library-nd.com 2023):

Fake or lying news (false or deceptive). This concept refers to information that is intentionally fabricated or manipulated to mislead readers or viewers (Gelfert 2018). This can include completely fabricated stories as well as news stories that have some element of truth but are distorted or taken out of context to support a particular agenda agendă (Baptista and Gradim 2022). One such example is the online rumor of the death (due to a heart attack) of George Soros on 05/15/2023, originally published on a Twitter account (@PoliticsFAIRL) and picked up by reputable accounts. The claim was not based on any real evidence (LaMagdeleine 2023).

Misleading information. Misleading articles are those that contain partially or completely inaccurate information or that are presented in a way that is designed to mislead readers or viewers (Zafarani, Zhou, et al. 2019). Unlike fake or deceiving news, misleading articles may contain an element of truth, but that truth is being

taken out of context or presented in a way that is designed to promote a particular agenda or point of view (Gelfert 2018). An example of this type of information is the one according to which the reform of the justice system in 2022 will lead to the undermining of the Constitutional Court, Romania will lose its sovereignty, the constitution will no longer be respected and Romanian justice will be conducted in Brussels, to the liking of the West. This misleading narrative was launched in the context of the debates on the justice laws of 2022. In reality, the amendment of the law on the status of judges and prosecutors did nothing but align the Romanian justice system with the European one, respecting the principle of the supremacy of European law (Veridica.ro 2022b).

Polarizing or biased content (slanted/biased). Polarizing or biased content refers to news articles or reports that are presented in a way that favors a particular point of view or agenda (Schia and Gjesvik 2020). The content that falls into this category is not necessarily fake. The news reports true information but does so in a biased manner. This type of partisanship can be political, ideological, or cultural and can manifest itself in various ways, including selective reporting, sensationalism, or the use of loaded language (Baptista and Gradim 2022). Polarizing content may reflect an entity's desire to sway readers' opinions in a certain direction, or it may reflect its attempt to create a memorable news story. Examples related to this type of content occur when only news featuring a certain ideology/political party is presented by a news channel and the others are ignored. Similarly, a political party can only be presented negatively. Another example of polarizing media can be given by an advertisement that supports unproven scientific data (Drew 2023).

Manipulated/modified data. This concept refers to text, images, or video that has been intentionally altered or edited in a way that misrepresents the original content. This may include the use of manipulated images, edited videos, or selective quotes taken out of context (Zafarani, Zhou, et al. 2019). This data is usually used to create false narratives or to support a particular agenda (Zellers, et al. 2019). A telling example of this type of fake information is the video recording created by „deepfake" technology in which the president of Ukraine asked his countrymen to surrender to Russia (The Telegraph 2022).

Humorous pieces of media (including all its forms such as satire, parody, or jokes) (Baptista and Gradim 2022). Such news is intentionally fabricated or exaggerated for comic effect (Figueira and Luciana 2017). Unlike fake or misleading news, humorous news is not intended to mislead or deceive, but rather to entertain. Satirical news may use humor to comment on social or political issues or to expose absurdity or hypocrisy (Gelfert 2018). Even though these types of news are not intended to deceive, they can sometimes be mistaken for genuine news, especially if they are shared out of context or without proper attribution (Schia and Gjesvik 2020). An example of satire is the news story published by the US media group The Onion, known for its humorous news content, „Jimmy Carter wins boxing match against

Jake Paul". This news story, while obviously fake due to the age difference between the former US president and the social media personality, contains an edited photo of the two and the content of the article is presented in the style of a boxing gala recap (the ONION 2023).

2.3. Classification according to impact and motivation. A classification that aims to be more exhaustive and takes into account the motivations behind the creators of the fake as well as indications of the possible impact that each type of fake information can have if it is distributed in an enabling environment has been compiled by the European Association for Viewers' Interests (EAVI) and contains a total of 10 categories classified according to impact (neutral, small, medium, large) and motivation (monetary, political/power, humor/entertainment, passion/ extremism or misinformation) (EAVI 2022):

Propaganda – used by governments, corporations, or nonprofit organizations to control attitudes, values, and disseminated information. This can be beneficial or harmful depending on the motivation behind the campaign which can be created to support a state policy or to create a negative sociopolitical state (neutral impact and motivation related to politics and passion)

Clickbait – offers sensational headlines that attract attention but are misleading because they do not reflect the written content of the material (low impact, motivated by money and entertainment value). Examples of clickbait headlines can be: "You won't believe...", "X things you need to know...", "A weird trick...", "This is what will happen if... ", "The best X...". Examples of this type of news are mostly found in the fashionable sections of the tabloids: "What does Bianca Drăgușanu say about her second child. "I have everything I need, for sure (Lixandru 2023)." From the point of view of disinformation, it is relevant that this type of headline can be used to spread campaigns containing false information.

Sponsored content – has a similar form to that of editorials but disguises ads without making it clear to consumers (low impact and monetary motivation). This type of advertising is considered harmful, especially among young people who cannot differentiate between disguised advertisements (sponsored content) and online normal news articles (McAlpine 2019).

Satire and Hoax – is a humorous social commentary that varies in quality and may have a subtle meaning (low impact and humorous motivation). This class is similar to the humorous pieces in the media (chapter 2.2) with the specification that usually these contents are polarizing/biased in favor of certain agendas.

Error – news or information containing false facts as a result of involuntary errors (the impact is reduced and the motivation is based on misinformation). This type of error can perpetuate false information by not verifying the original source.

Partisan - news that claims to be impartial, includes interpretations of the facts, has an ideological factor, and includes only the facts that confirm a position or policy, ignoring the others (ideological motivation and average impact). This type of news is used in propaganda campaigns to increase the level of credibility of the narratives presented. In such cases, genuine experts or pseudo-experts may be invited to support a point of view but claim impartiality. Partisanship was used during the 2016 US presidential election to so-called impartially create a positive image of one of the candidates (EAVI 2022).

Conspiracy theory – news that simplistically explains complex events as a response to fear or insecurity. These cannot be scientifically verified and the data that denies the respective theories is considered evidence that actually confirms the hypothesis (high impact, ideological motivation, or related to misinformation). Such theories were used during the COVID-19 pandemic to link the vaccine to 5G technology and the Microsoft corporation to create an anti-Western attitude.

Pseudoscience – news that supports theories such as miracle cures, the anti-vaccine movement, and misrepresents real scientific studies with exaggerated or false claims. (high impact, political or monetary motivation). Pseudoscience was used throughout 2020-2021 to promote various anti-EU narratives. Thus, a narrative taken from the eastern zone stated that the anti-Covid measures decided by the authorities are ineffective. The campaign to contest the sanitary measures taken to combat the SARS-CoV-2 pandemic continued in 2021 and pleaded for alternative treatments that did not receive the approval of the Romanian or European health authorities (Arbidol, Ivermectin) that were promoted by obscure doctors or influencers without medical training, at the same time contesting the effectiveness of anti-Covid vaccines employing pseudo-scientific data - either false information or some taken out of context. Of note during this period was the focus on adverse reactions to vaccines, realized through different medical professionals, usually with specializations that have nothing to do with virology, respectively by so-called experts in alternative medicine (Gomboș 2021).

Misinformation – includes a mix of real and fake information combined with false associations, processed content, and misleading headlines. Even if it aims to inform, the author does not know that the information used is false (high impact and motivation are to misinform). Disinformation usually involves concentrated action by different entities and has a clear purpose behind it, usually ideological or military. A famous disinformation campaign took place in World War II when the British government discovered the radar and did not want to tip the enemy about this fact. Therefore, they started a media propaganda campaign in the UK which created the myth that eating carrots helps develop night vision and the UK pilots benefit fully from this discovery (Smith 2013).

Bogus – content that is completely fabricated and spread with the obvious intent to misinform. This category may include guerrilla marketing tactics, software bots,

or fake comments. This content is intended to bring financial gain or political/ ideological influence (high impact, political or monetary motivation). For example, according to Meta's Q1 2023 Quarterly Adversarial Threat Report (Meta 2023), the company removed 40 Facebook accounts, 8 pages and one group for violating Meta's coordinated inauthentic behavior (CIB) policy. The identified network had its origin in Iran and mainly targeted Israel, Bahrain, and France, countries where it operated by posting probably fake ads to gain an increased level of authenticity and insert into established thematic forums on Facebook, Twitter, YouTube, or Telegram. The network could then have been used for various political or pecuniary purposes.

2.4. Lack of consensus. The presented classifications touch upon the problem of identifying and presenting false information from several perspectives. They contain common elements but do not completely overlap. Although the rankings of false information presented started from various differentiations such as intention, impact, and motivation, overlaps of meaning could not be avoided, but no universal classification and implicitly a categorical definition of different types of false information may result from them. Moreover, a unanimous definition is probably not a possibility in the near future due to the multitude of characteristics and diverse forms of manifestation that the creation and distribution of false information has.
The term fake news, although not found in all classifications, which is one of the most used in research and involves the categorization of false information obtained from the public space because it also involves verifying their veracity, is worth noting.

3. Classifying false information and creating datasets for research

The lack of a consensus regarding the definition of fake news and the multitude of sociocultural situations that give perspectives to this phenomenon is stated as one of the initial problems that need to be taken into account in the context of the use of artificial intelligence in the research of the creation and spread of false information. This difference in cataloging creates a problem that, although not obvious, becomes essential in the process of training AI models and testing them. The problem is given by the lack of data ready to be labeled with fake news. To solve this shortcoming, different online projects created data sets for research purposes. Such pre-labeled fake news datasets are collections of news where each piece of information, typically a news article or headline, has been labeled by a human operator as "true" or "false" (or in a variant with more tags) (ISOT Lab 2017). These datasets are used to train and evaluate machine learning models that can automatically classify news articles or headlines as true or fake based on patterns and features learned from labeled data (McIntire 2020).

Such datasets can be used to tune pre-trained language models, such as the Bidirectional Encoder Representations from Transformers (BERT) NLP model

(Ozbay and Alatas 2020), which have already been trained on large amounts of general text data. This can help the models adapt to the specific characteristics of the fake news dataset and improve their performance in identifying fake news (Devlin, et al. 2019).

The fake and real news datasets were constructed by research teams from real-world news articles that were previously vetted by media professionals (Wang 2017; Ahmed, Traore and Saad 2017). Such datasets are used to train and test different automatic fact-checking methods using AI models (Ozbay and Alatas 2020). The article will present some established data sets compiled from news stories that have been previously verified and labeled accordingly.

With the rise of disinformation campaigns, various fact-checking organizations or groups have come together in line with the goal of educating the public to discern true from false information presented by the media. Such examples may include PolitiFact, factcheck.org, or Snopes. Facebook even built its own „International Fact-Checking Network" (IFCN 2016) which has over 90 signatories from all over the world, including Romania.

Such fact-checking entities provide various types of fake news classification methods or annotations to record media verification. For example, PolitiFact takes current news from various outlets or media sources, verifies their claims using official sources or statistical data, and then assigns easy-to-use labels that show how true a media article is, using labels such as: mostly true, true, half true, mostly false, false, pants on fire (PolitiFact 2017); Snopes uses a similar tag code: true, mostly true, mostly false, false, outdated, scam, unproven (Snopes n.d.); the Romanian news verification organization, factual.ro, uses labels such as: true, partially true, truncated, false, impossible to verify (Factual 2016). All these groups base their claims on the percentage of true versus false information in the analyzed media article. It is relevant that fact-checking teams use only open-access sources during these checks.

Developing a fake news dataset typically involves a process of collecting, annotating, and validating news articles from various sources. An overview of the steps involved in creating a dataset of fake and real news from tagged news presented by media outlets includes collecting news articles from a variety of sources, including both traditional news outlets and alternative news sources (IFCN 2016). Next, articles should be checked for fake news content (Kaggle 2018). This is done by expert human annotators who review articles following a pre-set and transparent methodology. After identifying fake news articles, they are annotated with tags indicating whether they are real or fake (Factual 2016) by the same annotators. Finally, the dataset must be validated to ensure that it is reliable and accurate. This can be done by comparing annotation results with other data sources, such as fact-checking websites or other expert sources (Preda, et al. 2022).

By collecting news already tagged by these platforms, researchers involved in fake news studies are able to generate large datasets of certified fake and real news content without having to personally verify and tag them. The basis for labeling a news story is mainly based on the degree of false data that can be found in it. Because there is not yet a standardized way to label false averages and to address certain limitations that arise from using multiple labels for datasets, most established datasets use a binary classification for data, „False" and „True" and ignore labels such as mostly true, half true, or unverifiable.

An example dataset widely used in fake news research called ISOT (Ahmed, Traore and Saad 2017) contains over 1.2 million news articles in various languages, including English, Spanish and Portuguese, and comes from various fact-checking sources, covering a wide range of topics and fields. The dataset was created by the Information Security and Objects Technology (ISOT) Research Group at the University of Victoria in Canada (Ahmed, Traore and Saad 2017). Each news article in the dataset has already been checked by expert human annotators and is labeled as real or fake. Additional metadata such as source, author, and publication date are also provided within the data collection. The dataset is freely available for download and can be accessed via the ISOT Research Group website (ISOT Lab 2017).

A similar dataset used is PolitiFact's LIAR dataset (Wang 2017). PolitiFact is a nonpartisan fact-checking website that evaluates the accuracy of statements made by politicians, public figures, and other prominent individuals. It was founded in 2007 by the Tampa Bay Times, a newspaper in Florida, and has since expanded to include partnerships with other news organizations. PolitiFact rates statements on a „Truth-O-Meter" scale that uses categories ranging from „True" for real news stories to „Pants on Fire" for stories that contain no element of truth or have a nonsensical theme. The site provides detailed explanations and evidence for its ratings and aims to promote transparency and accountability in public discourse by helping people separate factual information from misinformation and propaganda. The dataset called „Liar, Liar, Pants on Fire" is verified by PolitiFact and consists of 12,836 statements made by politicians, which are labeled with six different labels: pants-on-fire[1], fake, barely true, half-true, mostly true, and true. The dataset was created to support research on automated fact-checking and fake news detection by being organized as a database containing the news or statement, information about the source of the statement, the person who made the claim, the context in which it was made, and fact-checking label assigned by PolitiFact (Wang 2017). It has been used to train and test machine learning algorithms for fact-checking and fake news detection and has been cited in numerous research studies (Wang 2017).

[1] "Pants-on-fire" - colloquial expression from the English language that comes from the nursery rhymes "liar, liar, pants, on fire!" meaning someone has been caught lying.

Another established dataset was compiled by KAGGLE and is known as the Kaggle Fake News Dataset (Kaggle 2018). It consists of a collection of news articles labeled either „Fake" or „Real" based on their accuracy and credibility. Kaggle is a popular platform in the field of data science and the organization of competitions involving machine learning technologies. The training dataset contains 20,800 news articles, and the test set contains 5,200 news articles, including a mixture of real news articles from reputable sources and fake news articles from unreliable sources. Fake news articles were collected from various sources on the internet and tagged by people based on their veracity. Real news articles have been collected from reputable news organizations and verified for accuracy by fact-checking organizations (Kaggle 2018). The dataset includes information about the title, text, author, and publication date of each article, as well as metadata such as the source URL and number of social media shares. The Kaggle Fake News dataset has also been used in numerous research studies and machine learning competitions and has helped advance the development of automated systems for detecting fake news.

Datasets such as those presented in this chapter allow researchers to fine-tune their models, focus on achieving superior performance, and more precisely define the classes that an AI model should consider when performing tasks related to identifying fake news, and misinforming content.

4. Using fake news datasets in research. Binary or multiclass approach

The data sets presented in the previous chapter allow the research approach from several perspectives: binary (true vs. false) or multiclass (true, partially true, neutral, etc.) In the process of automatic detection of fake news, a binary approach is a method where the machine learning algorithm is trained to classify news articles into two categories: fake or real (Kaliyar 2021). In contrast, a multiclass approach is a method where the algorithm is trained to classify news articles into more than two categories, such as partially true, completely false, and true, impossible to classify, true, satire, propaganda, etc. (Wang 2017).

A binary approach is commonly used in automated fake news detection because it simplifies the problem and makes it easier to manage. Instead of classifying news into multiple categories, a binary approach only requires distinguishing between two classes: real news and fake news (Chen, et al. 2017). This can help improve the accuracy of the classifier. In addition, as exemplified in previous chapters, the dataset was usually composed of only proven fake and proven real news and labeled by creators only in the two classes to avoid further interpretations (Kaggle 2018; ISOT Lab 2017). By choosing this binary approach the existing tagged data set can be used without the need to create any additional tags. This saves time and resources and allows researchers to focus on improving model performance on the two classes

of interest. In addition, a binary approach provides a clear and easy-to-understand result that can be useful to end users (Kaliyar 2021). For example, a news aggregator or social media platform may only need to know whether a piece of content is fake or not to decide whether to display it to users. A binary classifier can quickly provide this information, making it more useful for such applications (Ahmed, Traore and Saad 2017).

In addition, a binary approach can also simplify the evaluation of model performance. Established metrics to measure a model's effectiveness such as accuracy, precision, regression, and F1 score (another metric that measures model accuracy, combined with regression score) are easier to calculate and interpret when dealing with only two classes (Gnanambal, et al. 2018), this approach thus helping researchers to more easily compare and select the model with the best performance (Yerlikaya and Aslan 2020).

Conclusion

This article highlights the problem of managing fake news from the perspective of its research and some of the problems encountered in this regard. An initial problem concerns the identification of a common typology of false information. The initial use, including in legal texts, of the generic term 'fake news' is currently considered insufficient to encompass the entirety of the existing types of false information and is presently retained within the realm of research because its definition enables researchers to categorize a specific type of news conclusively, having undergone verification with no ambiguity about its classification. This type of approach cannot capture everyday reality in all its manifestations but it represents an initial step in the right direction because the resulting software product can, for example, be used in the rapid initial flagging of certain categories of false information or disinformation campaigns. The paper contributes to the existing literature on automated fake news detection by providing a framework for understanding and addressing this complex phenomenon. We hope that this paper can inspire research and innovation in this field, as well as become a source of information for policymakers and practitioners involved in disinformation management.

References

Ahmed, H., I. Traore, and S. Saad. 2017. "Detection of online fake news using N-gram analysis and machine learning techniques." *International conference on intelligent, secure, and dependable systems in distributed and cloud environments* 127-138. doi:https://doi.org/10.1007/978-3-319-69155-8_9.

Bahad, Pritika, Preeti Saxena, and Raj Kamal. 2019. "Fake News Detection using Bi-directional LSTM-Recurrent Neural nETWORK." *Procedia Computer Science* 165: 74–82.

Baptista, J.P., and A. Gradim. 2022. "A Working Definition of Fake News." *Encyclopedia* 632-645. doi:https://doi.org/10.3390/encyclopedia2010043.

Cezar, Nicholas. 2022. „De ce Războiul din Ucraina nu poate avea învingători." *Național.* https://www.national.ro/politica/de-ce-razboiul-din-ucraina-nu-poate-avea-invingatori-762950.html.

Chen, W., X. Xie, J. Wang, B. Pradhan, H. Hong, D. T. Bui, and J. Ma. 2017. "A comparative study of logistic model tree, random forest, and classification and regression tree models for spatial prediction of landslide susceptibility." *Catena* 151: 147-160. http://dx.doi.org/10.1016/j.catena.2016.11.032.

Devlin, J., M. W. Chang, K. Lee, and K. Toutanova. 2019. *BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding.*

Drew, Chris. 2023. "35 Media Bias Examples for Students." https://helpfulprofessor.com/media-bias-examples-for-students/.

EAVI. 2022. "Beyond Fake News – 10 Types of Misleading News." https://eavi.eu/beyond-fake-news-10-types-misleading-info/.

Emre, Celebi M., and Kemal Aydin. 2018. "Unsupervised Learning Algorithms." doi:https://doi.org/10.1007/978-3-319-24211-8.

ENISA, European Union Agency for Cybersecurity. 2022. "ENISA Threat Landscape 2022." https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

Factual. 2016. https://www.factual.ro/.

Figueira, A., and O. Luciana. 2017. "The current state of fake news: challenges and opportunities." *Procedia Computer Science* 121: 817-825. doi:https://doi.org/10.1016/j.procs.2017.11.106.

Gelfert, A. 2018. "Fake news: A definition." *Informal logic* 38 (1): 84-117. doi:https://doi.org/10.22329/il.v38i1.5068.

Gnanambal, S., M. Thangaraj, V. T. Meenatchi, and V. Gayathri. 2018. "Classification algorithms with attribute selection: an evaluation study using WEKA." *International Journal of Advanced Networking and Applications* 9 (6): 3640-3644. https://oaji.net/articles/2017/2698-1528114152.pdf.

Gomboș, Cătălin. 2021. „România 2021: Top FAKE NEWS & DEZINFORMĂRI demontate de Veridica." https://www.veridica.ro/stiri-false/romania-2021-top-fake-news-dezinformari-demontate-de-veridica.

IFCN, International Fact-Checking Network. 2016. "Verified signatories of the IFCN code of principles." https://ifcncodeofprinciples.poynter.org/signatories.

ISOT Lab. 2017. "ISOT Fake News Dataset." https://www.uvic.ca/ecs/ece/isot/datasets/fake-news/index.php.

Kaggle. 2018. "Fake News Detection." https://www.kaggle.com/jruvika/fake-news-detection.

Kaliyar, R.K., Goswami, A., and Narang, P. 2021. "FakeBERT: Fake news detection in social media with a BERT- based deep learning approach." *Multimedia Tools and Applications* (80): 11765–11788. doi:10.1007/s11042-020-10183-2.

LaMagdeleine, Izz Scott. 2023. "No, George Soros Is Not Dead." *Snopes.* https://www.snopes.com/fact-check/george-soros-is-not-dead/.

library-nd.com. 2023. https://library-nd.libguides.com/fakenews/categories.

Lixandru, Livia. 2023. „Ce spune Bianca Drăgușanu despre al doilea copil. «Am tot ce îmi trebuie, cu siguranță»." *Libertatea.* https://www.libertatea.ro/entertainment/ce-spune-bianca-dragusanu-despre-al-doilea-copil-4566539.

Magdin, Radu. 2013. „Constanța: locul unde se ciocnesc interesele. Internaționale." https://cursdeguvernare.ro/constanta-locul-unde-se-ciocnesc-interesele-internationale.html.

McAlpine, Kat J. 2019. "Most people can't tell native advertising apart from actual news articles, according to new research." https://www.futurity.org/sponsored-content-real-news-1961062/.

McIntire, G. 2020. "Fake News Dataset." https://github.com/pmacinec/fake-news-datasets/tree/eb85398bab558791c9f879e9f96ce72a471d2cc9.

Meta. 2023. "Quarterly Adversarial Threat Report Q1 2023." https://about.fb.com/wp-content/uploads/2023/05/Meta-Quarterly-Adversarial-Threat-Report-Q1-2023.pdf.

NATO Strategic Communications Centre of Excellence. 2020. "Defence Strategic Communications ." *Academic Jurnal Volume 8* (8). doi:DOI: 10.30966/2018.RIGA.8.

Necșuțu, Mădălin. 2022a. „Dezinformare: Majoritatea românilor vor ieșirea țării din NATO și UE." https://www.veridica.ro/dezinformare/dezinformare-majoritatea-romanilor-vor-iesirea-tarii-din-nato-si-ue.

—. 2022b. "Disinformation: The West is fighting Russia using Ukraine as proxy." https://www.veridica.ro/en/disinformation/disinformation-the-west-is-fighting-russia-using-ukraine-as-proxy.

Osborne, Hilary. 2017. "Revealed: Queen's private estate invested millions of pounds offshore." *The Guardian.* https://www.theguardian.com/news/2017/nov/05/revealed-queen-private-estate-invested-offshore-paradise-papers.

Ozbay, Feyza Altunbey, and Bilal Alatas. 2020. "Fake news detection within online social media using supervised artificial intelligence algorithms." *Physica A: statistical mechanics and its applications* 540. doi:https://doi.org/10.1016/j.physa.2019.123174.

Peiu, Petrișor. 2022. „Blocadă olandeză la porțile castelului Schengen. Pericolul naționalismului lipsit de inteligență." *Gândul.* https://www.gandul.ro/opinii/blocada-olandeza-la-portile-castelului-schengen-pericolul-nationalismului-lipsit-de-inteligenta-19860233.

PolitiFact. 2017. https://www.politifact.com/.

Preda, A., S. Ruseti, S. M. Terian, and M. Dascalu. 2022. "Romanian Fake News Identification using Language Models." doi:DOI: 10.37789/rochi.2022.1.1.13.

Radu, Cristina. 2022. „Antena 3 a prezentat din eroare imagini dintr-un joc video din 2013 ca fiind din războiul Rusiei împotriva Ucrainei." *Libertatea.* https://www.libertatea.ro/stiri/antena-3-a-prezentat-din-eroare-imagini-dintr-un-joc-video-din-2013-ca-fiind-din-razboiul-rusiei-impotriva-ucrainei-4005144.

Romanian Parliament. 1968. „Codul Penal din 21 iulie 1968 (**republicat**)." https://legislatie.just.ro/Public/DetaliiDocument/38070.

—. 2009. „Codul Penal din 17 iulie 2009, Legea nr. 286/2009." https://legislatie.just.ro/Public/DetaliiDocument/223635.

Rashkin H., Choi E., Jang J.Y., Volkova S., and Choi Y. 2017. "Truth of varying shades: Analyzing language in fake news and political fact-checking." *Proceedings of the 2017 conference on Empirical Methods in Natural Language Processing, EMNLP.* 2931-2937. doi:10.18653/v1/D17-1317.

Schia, N.N., and L. Gjesvik. 2020. "Hacking democracy: managing influence campaigns and disinformation in the digital age." *Journal of Cyber Policy* 5 (3): 413-428. doi:https://doi.org/10.1080/23738871.2020.1820060.

Smith, K. Annabelle. 2013. "A WWII Propaganda Campaign Popularized the Myth That Carrots Help You See in the Dark." *Smithsonian Magazine.* https://www.smithsonianmag.com/arts-culture/a-wwii-propaganda-campaign-popularized-the-myth-that-carrots-help-you-see-in-the-dark-28812484/.

Snopes, Snopes Media Group Inc. fără an. https://www.snopes.com/. Accesat 2 februarie 2023.

the ONION. 2023. "Jimmy Carter Wins Boxing Match Against Jake Paul." https://www.theonion.com/jimmy-carter-wins-boxing-match-against-jake-paul-1850487520.

The Telegraph. 2022. "Deepfake video of Volodymyr Zelensky surrendering surfaces on social media." https://www.youtube.com/watch?v=X17yrEV5sl4.

US Department of State. 2023. "Disarming Disinformation: Our Shared Responsibility." https://www.state.gov/disarming-disinformation/.

Veridica. 2022a. "Fake news: The Netherlands opposes Romania's Schengen accession because the port of Constanța threatens the supremacy of the port of Rotterdam." https://www.veridica.ro/en/fake-news/fake-news-the-netherlands-opposes-romanias-schengen-accession-because-the-port-of-constanta-threatens-the-supremacy-of-the-port-of-rotterdam.

—. 2022b. „Fake news: The reform of the justice system leads to the undermining of the Constitutional Court and Romania losing its sovereignty." https://www.veridica.ro/en/fake-news/fake-news-the-reform-of-the-justice-system-leads-to-the-undermining-of-the-constitutional-court-and-romania-losing-its-sovereignty.

Wang, W. Y. 2017. "«Liar, Liar Pants on Fire»: A new benchmark dataset for fake news detection." *Proceedings of the 55th annual meeting of the association for computational linguistics* 422-426. https://arxiv.org/abs/1705.00648.

Wardle, Claire, and Hossein Derakhshan. 2017. "Information Disorder: Toward an interdisciplinary framework for research and policy making." https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html.

WEF, World Economic Forum. 2023. "The Global Risks Report 2023." https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.

XIA, Xin, and LO, David. 2018. "Feature Engineering for Machine Learning and Data Analytics." *Feature* (CRC Press) 335-358. https://ink.library.smu.edu.sg/sis_research/4362 .

Yerlikaya, Turgay, and Seca Toker Aslan. 2020. "Social Media and Fake News in the Post-Truth Era." *Insight Turkey 22.2* 177-196.

Yuandong Luan, and Shaofu Lin. 2019. "Research on Text Classification Based on CNN and LSTM." *International Conference on Artificial Intelligence and Computer Applications (ICAICA).* doi:https://doi.org/10.1109/ICAICA.2019.8873454.

Zafarani, Reza, Xinyi Zhou, Kai Shu, and Huan Liu. 2019. "Fake News Research: Theories, Detection Strategies, and Open Problems." *KDD '19: Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining.* doi:https://doi.org/10.1145/3292500.3332287.

Zellers, R., A. Holtzman, H. Rashkin, Y. Bisk, A. Farhadi, F. Roesner, and Y. Choi. 2019. "Defending Against Neural Fake News." https://rowanzellers.com/grover.

Zhou, Z., H. Guan, M. M. Bhat, and J. Hsu. 2019. "Fake news detection via NLP is vulnerable to adversarial attacks." doi:https://doi.org/10.48550/arXiv.1901.09657.

No.2/2023, APRIL-JUNE
https://doi.org/10.53477/2284-9378-23-22

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Manifestations of security culture at national level

Daniel Ionel Andrei NISTOR, Ph.D. Student*

*Ministry of National Defence, Bucharest, Romania
e-mail: dan.nistor.rp@gmail.com

Abstract

We are moving towards a new security paradigm in which the predictability and stability of the system of international relations are directly impacted by global strategic rivalry, with a significant potential for rearranging the relationships between strategic players with global interests. The concept of security culture must be understood in this context, integrated into the security paradigm, and tailored to the dynamics of the international security environment, as it affects a variety of fields in addition to security, including the military, economic, socio-political, and cultural ones. Using several studies and opinion surveys conducted by public opinion polling institutions and, respectively, by non-governmental organizations, regarding the measurement of the security culture and the reactions to it, it is crucial to examine the relationship between security culture and hybrid threats, societal resilience, information warfare, cyber security, or emerging threats. It is also important to follow the evolution of the concept of „security culture" in Romania. Last but not least, this essay aims to examine the distinctive components of security culture from fields and action directions while also offering a number of suggestions for raising security culture in Romania.

Keywords:
security culture; resilience; strategy; security.

Preliminary considerations

Social dynamics and the evolution of the security environment require a thorough analysis not only of doctrines, strategies, and plans but also of the concepts themselves. We are moving towards a new security paradigm, with a high potential for reconfiguring not only relations among strategic actors with global interests, but also the system of international relations. Conflicts, crises, and tensions are not limited to certain areas and regions and, although separate, have a global reach. At the same time, their size and relevance are also determined by the domain of action, which is not only military or only economic or only political-social but can be found simultaneously in several of them, manifesting in all environments, from land, air, and sea to space and cyber. The escalation of the Ukrainian conflict, the hostility between China and Taiwan, North Korea's nuclear and ballistic tests, the tense relations between Israel and Iran, or the ongoing conflicts in Africa are just a few examples that demonstrate the need for a new strategy for fostering a culture of security and preparing a country to deal with the changes brought on by the evolution of the security environment. We get a complex picture that highlights how unstable and easily destabilized the international socio-political environment is, as well as how challenging it is to predict and foresee the positions of strategic actors on a global scale if we combine these situations with the COVID-19 Pandemic, the economic crisis, and the energy crisis.

The COVID-19 epidemic altered the social paradigm and compelled us to adjust to a new social reality that included isolation, travel limits, working from home, individual and collective health discipline, and controlled economic rationalizations, things that were previously difficult to imagine. It is not difficult to detect and foresee the social impact and political-social consequences at the level of Romanian society if we add the economic crisis (inflation, monetary policy), as well as the energy crisis, on top of these aspects, at least in terms of the national security dimension.

Beyond giving a brief overview of the concepts, their development, and current usage, this article's main goals are to highlight the significance of security culture, identify the distinctive aspects of Romania's security culture, from its fields and directions of action to its perceptions as measured sociologically, and offer a number of suggestions for raising the country's level of security culture. A multi-domain approach is necessary to fully understand security culture since it affects not just the security area but also the social, political, economic, and cultural domains.

1. Conceptual, diachronic approaches and manifestations of the security culture concept

A broader environment must be considered while examining security culture. Combining the phrases "culture" and "security" produced a brand-new idea with a

distinct meaning from the ideas explored independently. Although the concept of security culture seems more and more often associated with the fields of security, defense or cyber, it is important to remember that man and human nature are the most important elements to consider as security culture exists and manifests itself in every organization, even though it is not received and treated distinctly and most of the definitions refer to "ideas, customs, values and social behaviors that influence the security of a group" (Carpenter and Roer 2022, 30).

1.1. From culture and security to security culture

Durkheim (1933) defined culture as "the way a community thinks about itself in relation to the items that effect it" (Lincoln and Guillot 2004). Culture can be categorized sociologically into general, material, patrimonial, intellectual, or diversified knowledge in numerous domains. It can also be broken down into common behaviors, language, and communication, as well as values and beliefs. Security culture, as seen from a sociological angle, is "a culture of democratic resilience, an institutional culture that promotes the perception of institutional predictability and positive collective feelings, such as trust, optimism, and assertiveness" (Dumitrescu 2018a).

Barry Buzan comes up with a distinct approach to the concept of security and defines the concept of security as being "about the right to be free from threats and about the ability of states and societies to maintain their independence, identity and functional integrity against forces considered hostile who want to change it. The key to security is survival, but this also reasonably includes a number of concerns about existential conditions. The difficulty lies in the boundary between concerns that are attributed to security (threats sufficient to justify urgent action or exceptional measures, including the use of force) and those that are part of everyday uncertainties' (Buzan 1991, 432-433). Hama reinforces Professor Buzan's idea of linking the definition of security to "establishing the area of relevance", also emphasizing the 5 relevant sectors – political, military, economic, social and ecological - that can affect "the security of human collectives" (Hama 2017).

Piwowarski defines security culture as "a material and immaterial whole of elements of a consolidated heritage of people, intended to cultivate, recover (if it has been lost) and increase the level of security of individuals and collectivities". In this context, the author reviews the concept of culture, defined in 1871 by the anthropologist Edward Taylor, as a concept that includes "knowledge, beliefs, art, morals, laws, customs, as well as other capabilities necessary for a man, as a member of society" and arrives at the three "pillars of culture: individual, social and material", after analyzing "components of culture: material reality, social culture and ethical culture", defined in 1952 by Alfred Louis Kroeber (Piwowarski 2017, 17).

Buluc defines security culture as "the outcome of social interactions that take place in groups, organizations, communities, and societies concerned with aspects of social

security, which have in common certain learning and knowledge accumulation processes" in order to meet the needs of people in terms of trust, protection, and safety (Buluc, et al. 2019). Security culture must be understood as a living, evolving concept that responds to social change, is passed down through generations, and attempts to provide individuals the skills they need to not just identify threats but also to prevent them and learn how to respond to and neutralize them. The social milieu, the geostrategic and regional context, and the normative social structure all influence societal developments.

Security culture is defined as "the entirety of values, norms, attitudes, or actions that determine the understanding and assimilation at the level of society of the concept of security and its derivatives (national, international, collective security, insecurity, security policy, etc.)" in Romania's National Defense Strategy Guide from 2015 and here we also list the ideas connected to or deriving from the idea of security (presidency.ro 2015a).

According to Lesenciuc, security culture is "a set of norms, values, attitudes and behaviors resulting from a people's customs, traditions, symbols, and behavior patterns, which are in turn conditioned by the adaptation to the environment (including the response to threats), which ensures the understanding and assimilation of the concept of security and derived concepts (including the Security-freedom balance), the achievement and maintenance of a necessary minimum level of security" (Lesenciuc 2022, 124-141).

The shift from the two concepts of culture and security to the concept of security culture, which has a distinct meaning, preserved the norms, values, attitudes, and actions and integrated them into a pattern or model, determined the functional processes that develop state institutions' capacity to prevent and act, and helped people develop the skills they need to not only be aware of threats but also to prevent them and learn how to neutralize them.

1.2. Security culture and political culture

Traditionally, security culture may be thought of as conceptually descending from political culture. The renowned political scientists Sidney Verba and Gabriel Almond (1963) identified three categories of political culture: parochial, dependent, and participative after analyzing the cognitive, evaluative, and emotional attitudes of the populace toward politics and society (also called civic culture). According to Almond and Verba, "public participation in any form, but especially through association with others, trust in citizen competence, largely equivalent to participation (as opposed to dependent competence, which only requires knowledge and obedience to the law)" are guarantees of democratic stability (Bujder 2010). Because the security culture also shows itself in the political sphere and uses the same social and security values and norms, the political system can only continue to guarantee democratic stability if it is able to harmonize with the social, economic, cultural, and security

systems. Dumitrescu underlines that "both can be operationalized on the cognitive, evaluative, and emotional dimensions and arises from the experience of citizens with a more or less predictable institutional grid", emphasizing the connection between the political and security cultures (Dumitrescu 2018b).

1.3. Strategic culture and security culture

Jack Snyder first coined the term "strategic culture" in 1977 when researching how Soviet leaders differed from American ones in terms of culture and conduct during the Cold War. This idea is regarded as the forerunner to the term "security culture" (Lantis 2002, 87-113). The ideas put out by Snyder are adopted and developed by Colin S. Gray in his article *National Style in Strategy: The American Example* from 1981. Gray notes that the US, like Russia, has a unique strategic culture, which has important consequences for nuclear strategy. Strategic culture was described by Gray as a manner of "Thinking and behavior that are influenced by ideas about the nation's past and goals for self-definition (such as „Who am I as an American? How should I feel, think, or act?) and various American citizen-specific experiences (geographical, political, philosophical, and civic). Thus, geopolitical, historical, and economic experiences all contribute to the uniqueness of American strategic culture" (Zaman 2009, 68-88).

With a focus on the perception of the concept of security culture, we can conclude from an analysis of the definition that the influencing factors mentioned can particularize security culture in other geographic areas that are not strictly defined by state borders. For instance, an American will understand security culture differently than a Romanian, a Russian, or a Chinese due to different reference systems, in which norms, national values, experiences, and other factors differ.

1.4. Security and resilience culture

In the Global Strategy of the European Union from 2016, the term security is equivalent to that of resilience. In the view of Brussels, "the resilient state is a democratic state, which systematically produces trust in its own institutions and which ensures sustainable economic development. The resilient state diffuses, therefore, a culture of resilience, i.e. the perception of institutional predictability" (Mihai, et al. 2022).

Resilience is described as "the ability of an individual, a household, a community, a country or a region to prepare for, to resist, to adapt and recover quickly from situations of stress and shock, without compromising long-term development prospects" in the Communication "The EU approach to resilience: learning from food security crises. "The dual approach to resilience can be seen: the community and individual level, the ability of an entity to recover quickly from impact and the intrinsic strength of the person to better withstand stress or shocks (European Union 2012). The capacity for resilience can be found in other areas as well, and the EU has approved national recovery and resilience plans for its member states.

Through these plans, the states can implement reforms and investments aimed at reducing the socioeconomic effects of the COVID-19 pandemic crisis, facilitating the nation's transition to a greener, more digital economy, or putting more of a focus on the needs of young people by bolstering the education sector (EPRS 2022).

Within NATO, the concept of "resilience" has also seen two approaches. The NATO Treaty (signed in Washington, 1949) emphasizes, in Article 3, the resistance capacity of each state "in order to be more effective in achieving the objectives of this Treaty, the parties, separately and together, through their own forces and mutual aid, will maintain and develop individual and collective ability to withstand an armed attack" (NATO 1949). At the 2016 NATO Summit, the approach to the concept of resilience and the need to strengthen it, considered the alteration of the security environment following the aggressive actions of the Russian Federation in Ukraine from 2014 "a necessary foundation for credible defense, deterrence, and efficient performance of the Alliance's core task". According to the hybrid threat model, resilience is defined as "the capacity of a government to continue functioning, to continue maintaining the delivery of services to the population, and to also continue providing civilian support for military operations". Regarding the need to build resilience, seven fundamental areas are specifically targeted: the continuation of government and essential government services; energy supply; the capacity to deal with the unrestrained movement of people; the management of water and food resources; the capacity to deal with catastrophic losses; the operation of telecommunications and cybernetic networks; and the viability of transportation systems (NATO 2016b). Resilience is a national obligation and a shared commitment, as the Madrid Summit underlined. "We are boosting our adaptability, in part through nationally determined targets and execution plans that are driven by goals created in collaboration with Allies. Additionally, we will improve our energy security" are the components spelled out in the final declaration, which all heads of state signed (NATO 2022).

So, through a security culture planned at the national or allied level with civil society input, resilience is either generated or strengthened. Through the process of educating and increasing public awareness, security culture can significantly boost resilience in areas like security, social cohesion, and political stability, implicitly supporting the maintenance of institutional stability (state or alliance of states).

1.5. Security culture and information warfare

One of the effective battle strategies Sun Tzu outlined in The Art of War was the eradication of resistance and the destruction of the enemy's will to fight. "An operation carried out to obtain an information or cognitive advantage over the adversary and consists of controlling one's own information space, protecting access to one's own information, while also acquiring and using the adversary's information, destroying his information systems, and disrupting the flow of information", according to the definition of information warfare (NATO 2016a). Although information warfare is not a new phenomenon, it has creative components

due to technological advancement, which makes information spread more quickly and on a larger scale.

By "projecting an alternate reality onto an established target population to create a perception of the target group that allows pressure on decision makers and the alteration of well-considered, evaluated, and strategically planned decisions relate to a narrow, concrete, delicate, and important subject related to the topic on which the alteration of the decision is desired" (Chifu 2022). Therefore, whether the goal of the impact is to change a strategic choice or create a destabilizing scenario, the efficiency of information warfare is also tied to the degree of security culture of the population, which can be targeted and acted upon to shift perception. An atmosphere that is favorable to information warfare tactics might be produced by a low-security culture.

1.6. Security culture and hybrid threats

The term "hybrid threats" refers to a group of "coercive and subversive tactics, conventional and non-conventional strategies (such as diplomatic, military, economic, and technological) that can be coordinated by state or non-state actors to achieve particular goals while staying below the threshold of the state of war. Typically, the goal is to impede decision-making processes by exploiting the target's weaknesses and creating ambiguity" (Frunzeti and Bărbulescu 2018, 16-26).

Combining the old information war weapons of propaganda, disinformation, and fake/fake news in a new and inventive way, hybrid threats weaken the line of the terrain of conflict between the actors. The Internet has supplanted the physical world as the place where action, impact, and influence are needed. Campaigns to spread misinformation are increasingly using social media to coordinate threats and hybrid activities, radicalize potential participants, and dominate political discourse.

Frunzeti lists the elements included in a study carried out by three institutions from Finland, Romania, and Sweden that "to the creation of hybrid threats": "The post-Cold War international order has changed; globalization, advanced communication technologies, and explosive changes in the online environment essentially contribute to increasing the action potential of state actors, but also of non-state actors; utilizing the potential offered by new media technologies as well as new tools for social influence" (Frunzeti and Bărbulescu 2018, 16-26). Since social influence tools are "double-edged weapons," they can both exploit the effect on the vulnerable population and help to increase the level of preparedness and resilience of the population by providing quick and affordable means of informing it. This is why the need for a security culture is a factor that has the potential to reduce these kinds of threats.

1.7. Security culture, cyber security, and emerging technologies

The evolution of the technological field also determines, implicitly, the diversification of threats and security risks that will increase the uncertainty and volatility of the global security environment, becoming more and more difficult to anticipate and counter. "Cyber attacks, activities specific to the information field (actions of

influence in the public space, disinformation generated by fake news), emerging technologies (5G, artificial intelligence, big data, cloud computing), threats to critical infrastructures, communications, transport and trade can lead to the emergence of interconnected risks and threats; the risks, the need for data protection and user education "complement" the beneficial effects generated by these technologies for citizens and the business environment. Drone technology (UAVs) has dramatically changed the shape of warfare and created a constant impact on the psyche of democratic societies." These types of capabilities, that threaten military security, may have a terrorist use or may affect critical infrastructure, energy security, or may be used for surveillance or influencing actions on specific targets (Chifu 2022).

Mihai notes in the report on the strategic resilience of the European Union that a number of crucial industries, including transportation, energy, health care, and finance, have become more and more reliant on digital technology to carry out their fundamental functions. "Despite the fact that digitalization presents the European Union with several chances and answers, such as during the Covid-19 pandemic crisis, it also exposes the business and society to cyber attacks. Around the world, cyber attacks and computer crime are becoming more frequent and sophisticated, and it is anticipated that this trend will continue to develop in the future" (Mihai, et al. 2022).

Social media has fundamentally altered how people interact by providing free access to "unlimited" knowledge and, at the same time, allowing some groups of people to exert influence over others in specific locations and on particular themes, which can quickly lead to polarization and radicalization. "The first requirement is to produce a comprehensive national policy for cyberspace and social networks," stressed Harlan Ullman, referring to US strategy and policy on the two topics, emphasizing the sanitization of cyberspace through government action and corporate and citizen accountability (Ullman 2021). This is precisely why a high degree of security culture can help reduce societal vulnerability by educating citizens to understand the nature of threats, learn to differentiate and verify the information before sharing or accessing malicious or disruptive IT content, resulting in thus a decrease in the degree or pace of influence actions.

1.8. Security culture and human security

Human security is extremely important, having in the foreground, the citizen and his safety, with a growing emphasis on the involvement of civil society in the process, starting from the assumption that a precarious security culture is a societal vulnerability. Understanding the role of each element contributing to social action from the state, public institutions, non-governmental organizations or corporations is important for understanding the role of the individual (citizen) in ensuring national and international security. Social security is represented by legal regulations designed to ensure the state of social security at the level of a person, social group or

total population, as well as to protect disadvantaged or marginalized people. Human security believes that "the health of the population is of paramount importance for the state's ability to survive within the international system" (Curos 2021, 40-47). Kay Roer emphasized the idea that people are different, with different needs and with a certain level of understanding, knowledge and the key to success in building, maintaining and growing a very good security culture is understanding these differences and the need to adapt the effort to their needs, to the context and their level of understanding and knowledge (Roer 2015). Emerging technologies, cyber threats, and information war are factors with disruptive potential in our activity, on a social or institutional level, but the common denominator and the most important factor in this equation remains the human factor. "In managing security and threats to it, the most problematic are individuals. Despite the existence of various forms of hardware and software, people are the ones who generate security breaches" (Brânda 2018). Precisely because of this, the security culture is the one that puts the individual in the center of attention and becomes a tool through which the citizen/ the human/ the individual reduces his risks and maintains a high level of societal integration and functional social relations.

1.9. Security culture and the multi-domain approach

The society's or organization's security culture is correlated with the areas in which it is applied or manifested. Techniques and strategies of action that are unique to the information war, which at first was mostly in the military or broad field, are also to be found in fields with no direct relationship to security, in the sense of the restricted definition of the term with application to the sphere of defense. Although international organizations (NATO, EU, OSCE) and states started to develop strategies and plans to implement resilience after the conflict in Ukraine in 2014, the concept of security culture remained in the strategic planning documents because there were few elements of its concrete application, with the emphasis being on applicability in the economic, social, energy, educational, cyber, or nuclear fields.

The activities of some entities, whether state actors or non-state players, can have ramifications and reverberations in many other domains and even cause large-scale effects that may result in crises of a social, socio-political, economic, or cultural-religious nature. The low level of security culture can be a risk factor or a catalyst for destabilizing events at the socio-political or security level. One example of this is societal resistance to disinformation.

2. Romanian security culture's outward manifestations

The security culture is expressed through social norms, beliefs, and attitudes that represent the society in which it exists and is projected in accordance with how those social norms are used in that particular society. During the communist era, Romanian values changed; the state assumed ownership of all property, and the

society was thought to be egalitarian, devoid of social class distinctions. At the same time, however, freedom of expression was constrained, and access to information was under the control of the state. The security culture was restricted to safeguarding the state and the values it imposed as well as the physical safety of the citizen, which depended heavily on a high level of adherence to the social norms the state imposed.

The security culture was restricted to safeguarding the state and the values it imposed as well as the physical safety of the citizen, which depended heavily on a high level of adherence to the social norms imposed by the state. After the system changed in 1989, there was a paradigm shift that resulted in a chaotic immersion in the concept of democracy, spurred on by an enthusiasm for the "abolition" of restrictions on free speech, the restoration of property rights, and unfettered freedom of choice. Romania's security culture aspired to follow a similar path to that of security and defense processes, with an effort to specifically adapt to the national transition for integration into the European and Euro-Atlantic course.

2.1. Evolution, manifestation and normative framework of the security culture in Romania

Analyzing the period before 1990, Cristian Felea (2018) presents Romania's security culture as "a value imposed by the communist leaders, only that it was defined differently, namely as revolutionary vigilance and as socialist ethics, through which "awakened social consciousness was formed " of every citizen of the communist state. Faced with such a perspective, which was inoculated to citizens from the earliest age (let us remember, the institutionalization of education implied the existence of civic-political education organizations, including at the level of preschool education, through the "falcons of the homeland"), it was expected from the active individual not to make any concessions from the prescriptions of the ethics which was called revolutionary consciousness" (Felea 2018). The adherence of Romania to European and Euro-Atlantic principles led to an adoption of the concepts of security, democracy, and the rule of law. This was followed by actual state changes in the majority of areas, including economics, politics, the military, and the legislative branch.

A first attempt to shift the national security issue's center of gravity to the level of the citizen, abandoning worries about state security, may be seen in Romania's National Security Strategy from 1999. This document presents a novel interpretation of the idea of national security from at least two angles. First of all, for the first time, the idea of national security is based on the citizen, on his fundamental interests and rights, rather than the state. According to Constantinescu, "In place of the old, centralized vision, a new idea has been placed, that according to which national security starts from guaranteeing a proper future for every human being." This new way of thinking helped to pave our country's path to the European Union, from the revision of the Constitution to accession and integration (Constantinescu 1999).

The National Defense Strategy for the period of 2015–2020 included a direction of action that aimed to incorporate security culture into the concept of national security: "The development of the security culture, including through continuous education, which promotes the values, norms, attitudes, or actions that allow the assimilation of the concept of national security." (presidency.ro 2015b).

The National Strategy for the Defense of the Country for the period 2020-2024 (Strategy) proposes an integrated management of risks and threats by the Romanian state, both nationally and internationally, with the fulfillment of Romania's responsibilities, as a member of the EU, NATO, OSCE, UN. "From the perspective of Romania's security, we must have a tailored and effective response to the risks, threats, and vulnerabilities we confront, based on continuity, adaptation, flexibility, resilience, and predictability" (presidency.ro 2020, 5).

Summarizing what has been presented, it can be said about the concept of security culture that, diachronically, it supports the idea that the central element, in Romanian society, is the citizen - integrated in the "state-society-citizen triad"– and we also find in the programmatic documents the recommendation to protect and promotion of national security values, emphasizing, at the same time, the necessity and importance of society's involvement in the process, being aware of the interdependence between the level of citizens' security culture and the stability, strength and resilience of a state.

2.2. Domains and directions of action specific to security culture

Analyzing the concept of security culture through the prism of the fields of manifestation: political, military, economic, social, information, an overlap can be achieved on the directions of action established for the implementation of the strategy, being correlative, according to the concept of extended national security and aimed at: "defense, diplomatic, information, counter-intelligence and security dimensions, public order, crisis management, economic and energy, societal dimensions" (presidency.ro 2020, 37).

Taking into account the significance of the goals, the directions of action for each aspect of achieving national security will be implemented with the following goals: "consolidating the national defense capacity; improving the effectiveness of national crisis prevention and management systems; strengthening the security of critical infrastructures; sustainable development of large public systems (health, education, social protection); the promotion of national identity (presidency.ro 2020). Regardless of whether we are discussing asymmetric or hybrid threats, emergencies or crisis circumstances, all of these orientations, aims, and methods are intended to defend the state and the citizen by assuring the state's resilience.

The social domain is where security culture has the biggest impact on security, and destabilizing variables can be produced by asymmetrical demographic change, the rise of individualism and isolation in cyberspace, and the susceptibility of online

social media to information warfare tactics. The crisis at the nation's borders, which was brought on by Russia's aggression against Ukraine, also brought to attention the implications of migration and refugee issues on regional and national security. The institutional approach to managing Ukrainian migrants has greatly decreased the security risk, but changes in the region's condition could make the issue worse.

The citizen is the subject on which action is taken in the cognitive-behavioral dimension in order to determine an appropriate response, either to accept situations, or to determine a contrary answer. The online environment and social networks must be approached separately, the social impact analyzed on all levels, interrelated with the other fields.

2.3. The perspective of security culture in Romania: studies, evaluations, and recommendations

To be able to adapt and correctly apply policies, measures, and actions at the level of institutions and the state, at the same time, they build and streamline a two-way communication and citizen involvement in the process of strengthening the security culture; it is crucial to understand how the security culture is perceived at the citizen and society level.

We analyzed the reports and studies on the security culture in Romania and, in 2018, three studies were highlighted that we will mention below, other studies that separately treat the field of security culture were not repeated and updated. In order to have a broader understanding of the phenomenon, we expanded the analysis and included studies and surveys that measured the level of security and specific parameters, studies carried out by Strategic Thinking (2022), the Romania 2050 Agenda project and the Laboratory for the Analysis of Information War and Strategic Communication, Security Barometer of Romania (LARICS 2022).

The Security Culture Barometer, the first sociological study to measure the idea of security culture in relation to the culture of insecurity, in antagonistic parameters, was introduced by the Laboratory for the Analysis of Information Warfare and Strategic Communication (LARICS) in 2018. It has seven dimensions with significant polarities for the survey topic: trust/distrust, localism/globalism, realism/liberalism, optimism/pessimism, security/rights, involvement/apathy, and many more. protection in Romania (LARICS 2018a).

Lungu, Buluc, and Deac have published a report on the perception of the promotion of the security culture, evaluating the approaches and strategies for doing so, as well as methods for piqueing the interest of citizens in this area. They also mention institutions that have a role to play or have the potential to do so. Although the PROSCOP survey, sociologically speaking, is not representative because the achievement sample is small (152 people), made up of students and pupils (73 %), from the urban environment (90%), the combined findings present a number of

recommendations for the actors responsible for the management of areas involved in the promotion of security culture, applicable at least to respondents who fit into the categories examined (Lungu, Buluc and Deac 2018).

On the other hand, Strategic Thinking carried out, in 2022, through the *Agenda Romania 2050 Project*, a series of sociological studies on six major areas of interest for the future of Romania, from infrastructure, health, education, climate change, to taxation, energy, digitization, security, etc. and the results indirectly confirm the results of the LARICS (2018b) survey on security culture, but also those of 2022 from the Security Barometer of Romania (LARICS 2022).

In this sense, from the analysis of the data of the LARICS barometer, the conclusion is that "Romanians are rather distrustful (56.6%) of institutions than confident (31.6%), they are oriented towards localism (48%) rather than globalism (36%), with a relative balance between focusing on rights (45.7%) and focusing on security (41.1%), more involved (52%) than apathetic (35%), but also a rather conspiratorial perspective (52.5%) on politics, the media and international relations than a rationalist one (32.3%)" (LARICS, Barometrul culturii de securitate partea 1 2018).

The Strategic Thinking study (2022) emphasizes a very important element that emerges from the socio-demographic analysis related to young people up to 30 years of age who believe, in higher percentages than the rest of the population, that NATO will remain Romania's main security guarantee. This highlight confirms the results of the PROSCOP study which pointed out that more than two thirds of respondents (69.7%) are aware of security risks, threats and vulnerabilities as the main objective in promoting security culture. About a third of the respondents believe that the promotion of the security culture should lead to the application by citizens of the norms, rules, standard procedures of action in the field of security (35.5%) or to the adaptation of individual and group behavior, as well as of the entire company to the specific conditions regarding security (30.9%).

"Although mistrust in institutions is dominant, there are no significant socio-demographic faults in the Romanian population from the point of view of the security culture, and the security-rights dimension is not as important for the structuring of security cultures as it seems to be in the public debate Romanian society; the three types of security cultures are dominated by conspiracy and vulnerable to fake-news". An extremely important positive element resulting from this study is that localist tendencies are not, for now, in contradiction with sympathy towards the EU/NATO (LARICS 2018a), elements also confirmed by the Strategic Thinking survey (2022) where in the opinion of 83.5% of Romanians, the WEST (i.e. EU, USA, NATO) is the direction Romania should go in terms of political and military alliances. In contrast, 8% believe that Romania should move towards the CEST (i.e. Russia, China), and 65.8% of Romanians believe that NATO will remain Romania's main security guarantee (StrategicThinking, 2022); the same element of certainty that "Romania's

population remains pro-Western and pro-European" is also emphasized in October 2022 by the LARICS study: 68% of respondents are optimistic about the future of the European Union in the short term, 78% are optimistic regarding American support for Eastern Europe and only 10% of Romanians believe that the EU should disappear in the future (LARICS 2022). Although the young public, educated in security (PROSCOP) believes that state institutions with attributions in the field of security and defense should have the main role in promoting security culture (71.1%), in the framework of the socio-demographic analysis (Strategic Thinking) it turned out that there are no significant differences according to the socio-demographic categories analyzed between those who believe that Romania should move towards the WEST from the point of view of political and military alliances, and from the point of view of security, 70.9% of Romanians believe that in the future the Romanian Army should increase, while 23.2% are of the opinion that the Romanian Army should remain as it is now and only 3.5% that it should reduce its numbers.

To sum up, the effective promotion of the security culture is closely related to the setting of priorities regarding the conceptual components of security, from dimensions to components, risks, threats, and vulnerabilities, against which particular courses of action and responses are designed, on the dimensions of security and defense, educational, health, social, and economic.

Conclusions

The risks and threats to the safety of the citizen and the state have, for some time now, transcended geographical boundaries, and security is no longer confined to the military. Instead, it now necessitates a multidisciplinary, interinstitutional approach, collaboration between governmental and non-governmental organizations, and a shift from the action of a few institutions and small groups to the entire society, with the preservation of personal safety as the main objective.

The paradigm shift brought about by Russia's aggression against Ukraine also influenced how the European Union would respond and how NATO would adjust its defensive and deterrence posture there. Although it is mentioned in the planning documents, the concept of security culture has not benefited from and does not appear to profit from a pragmatic approach of application, which was highlighted by the concept reset. The security culture needs more time to solidify as a distinct notion after the terms have been defined and the distinguishing aspects have been described. Although Romania has a national strategy (SNAT 2024) that places the citizen and his well-being at its center, the perception of the citizen does not align with this stated intention, so it must be understood, transposed, and integrated into a concrete way of action in strategies and plans. This requires expanding from the field of security and defense to other fields: from economic to social and educational.

https://doi.org/10.53477/2284-9378-23-22

In a consolidated democracy, safeguarding citizens must be at least as vital as protecting the state because state security is a fundamental component of society. Even though this is more difficult to accomplish in Romania due to the country's relatively high levels of institutional mistrust (56.6%) and conspiratorial views on politics, the media, and international affairs (52.5%), the effort needs to be refocused on the individual citizen in order to foster the growth of his security culture.

Since the Internet and television are viewed as conspiratorially, irrationally, emotionally, and without serious consideration of the sources, it is crucial that the state institutions learn to minimize risks and vulnerabilities and ensure prevention in order to be able to narrow the perception gap of the Romanian citizen. Another factor that raises the level of security culture is education, institutional cooperation, and civil society participation in the educational process. The development of a security culture and the ability of citizens to understand the risks, challenges, and threats to security both contribute to the widest possible public having a minimum level of knowledge about the concept of security. These two factors also directly influence actions to recognize and combat the effects caused by the phenomenon of disinformation. Along with strategy and resources, the main component in promoting security culture is the utilization of professionals in the sector. Institutions in charge of education can use training techniques and practical actions, such as conferences, debates, partnerships with academic or research institutions, meetings with pupils and students from educational institutions of all levels, introduction to school-level courses on the development of security culture, and meetings with representatives of the civil society.

At the national level, the security goals must be linked to the directions of action, the institutions must coordinate their work processes, act simultaneously and with coherence, support the updating of the law, ensure institutional transparency, and keep the citizen in mind as the primary stakeholder in maintaining the state's functionality. The security culture is presented as a way to be aware of risks, threats, and vulnerabilities and eventually to learn management techniques, not to prevent their occurrence. To change the attitude from the passive mode of response and countermeasures to the proactive mode of prevention, an institutional approach is required. Vulnerabilities can be prevented from becoming security threats by educating the public and fostering a strong security culture.

The state can protect society by enforcing its security policy, but by enhancing the security culture at the societal level, it can significantly lower risks and vulnerabilities in almost all areas because the effort will be collaborative rather than the result of the state acting alone and expecting a passive response from its citizens. To safeguard the government and its inhabitants, it is important to prioritize the security culture that education has helped to create.
A brief introduction to a PhD study with the title „Strengthening security culture through institutional strategic communication" is provided in this article.

References

bancherul.ro. 2021. „Plățile cu cardurile au crescut cu 60% în timpul pandemiei." https://www.bancherul.ro/stire.php?id_stire=20942&titlu=platile-cu-cardurile-au-crescut-cu-60-la-suta-in-timpul-pandemiei.

Brânda, Oana-Elena. 2018. „Cultura de securitate în organizații. Principii și dezvoltare." *Conferința națională științifică a Academiei Oamenilor de Știință „Cercetarea științifică în serviciul dezvoltării durabile.* Târgoviște: Academia Oamenilor de Știință.

Bujder, Irina. 2010. „Societatea civilă românească între performanţă şi participare publică." *Sfera politicii* (144). https://revistasferapoliticii.ro/sfera/144/art02-bujder.html.

Buluc, Ruxandra, Ioan Deac, Răzvan Grigoras, and Ciprian Lungu. 2019. *Cultura de securitate și fenomenul Fake News.* București: Editura Top Form.

Buzan, Barry. 1991. "New Patterns of Global Security in the Twenty-first Century." *International Affairs* 67 (3): 432-433.

Calangea, Claudia-Diana. 2017. „Cultura de securitate. Surse şi resurse". *Intelligence în serviciul tău.* https://intelligence.sri.ro/cultura-de-securitate-surse-si-resurse.

Carpenter, Perry, and Kai Roer. 2022. *The Security Culture Playbook.* John Wiley & Sons Inc.

Chifu, Iulian. 2022. *Reconfigurarea securității și relațiilor internaționale în secolul 21.* București: ISPRI.

Constantinescu, Emil. 1999. „Mesajul preşedintelui Emil Constantinescu adresat Camerelor reunite cu ocazia prezentării Strategiei de Securitate Națională a României." https://constantinescu.ro/discursuri/313.htm.

Curos, Ludmila. 2021. „Cultura de securitate dezvoltată prin educație." *Revistă științifico-practică nr. 1/2021 Jurnalul de relații internaționale, Moldova*, 40-47.

DEXonline. a. *cultură.* Accesat 25 ianuarie 2023. https://dexonline.ro/definitie/cultură.

—. b. *securitate.* Accesat 25 ianuarie 2023. https://dexonline.ro/definitie/securitate.

Dumitrescu, Lucian. 2018a. „Barometrul culturii de securitate." București: LARICS.

—. 2018b. „Lansarea barometrului culturii de securitate. Ce este cultura de securitate?" https://adevarul.ro/blogurile-adevarul/lansarea-barometrului-culturii-de-securitate-ce-1856753.html.

EPRS, Serviciul de Cercetare al Parlamentului European. 2022. „Planul național de redresare și reziliență al României." https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733641/EPRS_BRI(2022)733641_RO.pdf.

European Union. 2012. „Abordarea UE în materie de reziliență: să învățăm din crizele în domeniul securității alimentare." Bruxelles: Comunicarea Comisiei către Parlamentul European și Consiliu COM/2012/0586 final.

Felea, Cristian. 2018. „Cultura de securitate, semnul unui spațiu al civilizației și democrației." https://www.contributors.ro/cultura-de-securitate-semnul-unui-spațiu-al-civilizației-și-democrației.

Frunzeti, Teodor, and Cristian Bărbulescu. 2018. „Reziliența națională la amenințările hibride și cultura de securitate. Un cadru de analiză." *Impact Strategic* (nr.1/2): 16-26.

Hama, Hawre Hassan. 2017. "State Security, Societal Security, and Human Security." *Journal of international Relations* 21 (1). doi:https://doi.org/10.1177/0973598417706591.

Kemp, Simon. 2022. "Digital 2022: Global overview report." https://datareportal.com/reports/digital-2022-global-overview-report.

Lantis, Jeffrey S. 2002. "Strategic Culture and National Security Policy." *International Studies Review* 4 (3): 87-113.

LARICS. 2018a. „Barometrul culturii de securitate partea 1." https://larics.ro/wp-content/uploads/2018/04/Raport-sondaj-INSCOP-barometru-LARICS-partea-1.pdf.

—. 2018b. „Barometrul culturii de securitate partea 2." https://larics.ro/wp-content/uploads/2018/04/Raport-sondaj-INSCOP-barometru-LARICS-partea-2.pdf.

—. 2018c. „Neîncrederea în instituții domină cultura de securitate a românilor." https://larics.ro/neincrederea-institutii-domina-cultura-de-securitate-romanilor/

—. 2022. „Barometrul de securitate al României." https://larics.ro/barometrul-de-securitate-al-romaniei/.

Lesenciuc, Cozmanciuc. 2022. „Cultura de securitate – încercare de operaționalizare conceptuală pe coordonate constructiviste." *Gândirea Militară Românească* (1): 124-141.

Lincoln, Lames R., and Didier Guillot. 2004. "Durkheim and Organizational Culture." *IRLE Working Paper No. 108-04.* https://irle.berkeley.edu/files/2004/Durkheim-and-Organizational-Culture.pdf.

Lungu, Ciprian, Ruxandra Buluc, and Ioan Deac. 2018. *Promovarea culturii de securitate: raport.* București: Top Form.

Mihai, Ioan-Cosmin, Petre-Dan Cîmpean, Sabin Popescu, and Alina-Camelia Vasilescu. 2022. „Reziliența strategică a Uniunii Europene, inclusiv în domeniile tehnologic și digital: scenarii de viitor și contribuții ale României." Studiul nr. 2. http://ier.gov.ro/wp-content/uploads/2022/03/SPOS-2021.-Studiul-2.-Rezilienta-strategica-a-Uniunii-Europene_final_site.pdf.

NATO. 1949. „Tratatul NORD-ATLANTIC." https://www.mae.ro/sites/default/files/file/pdf/TRATATUL%2520NORD-ATLANTIC.pdf.

—. 2016a. "Information Warfare." https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf.

—. 2016b. "Warsaw Summit Communiqué." https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

—. 2022. „Declarația Summitului NATO de la Madrid." https://www.mae.ro/node/59136.

Piwowarski, Juliusz. 2017. "Three Pilars of Security Culture." *Security Dimensions* (No.22): 16-27. https://www.researchgate.net/profile/Juliusz-Piwowarski/publication/323243164_Three_Pillars_of_Security_Culture/links/5a883550458515b8af91b64f/Three-Pillars-of-Security-Culture.pdf, accesat la 24 iul 2022.

presidency.ro. 2015a. „Ghidul Strategiei Naționale de Apărare a Țării pentru perioada 2015-2019." https://www.presidency.ro/ro/presa/securitate-nationala-si-aparare/ghidul-strategiei-nationale-de-aparare-a-tarii-pentru-perioada-2015-2019.

—. 2015b. „Strategia Națională de Apărare a Țarii pentru perioada 2015-2020." https://www.presidency.ro/files/userfiles/Ghid_SNApT_2015-2019_AP.pdf.

—. 2020. „Strategia Națională de Apărare a Țării pentru perioada 2020-2024." https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf.

Roer, Kai. 2015. *Build a Security Culture.* IT Governance Publishing.

StrategicThinking. 2022. „Sondaj de opinie. Proiect: AGENDA ROMÂNIA 2050. O conversație despre viitorul României." https://www.strategicthinking.ro/iulie-2022-sondaj-de-opinie-proiect-agenda-romania-2050-o-conversatie-despre-viitorul-romaniei/.

Ullman, Harlan. 2021. *Al cincilea cavaler al apocalipsei și noul MAD.* București: Editura Militară.

Zaman, Rashed Uz. 2009. "Strategic Culture: A «Cultural» Understanding of War." *Comparative Strategy* 28 (1): 68-88. https://www.tandfonline.com/doi/full/10.1080/01495930802679785.

No.2/2023, APRIL-JUNE
https://doi.org/10.53477/2284-9378-23-23

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

The actions of the Russian Federation from the perspective of individual responsibility

Dragoș-Adrian BANTAȘ, Ph.D.*
Sebastian BĂLĂNICĂ, Ph.D. Candidate**

*"Carol I" National Defence University; „Nicolae Titulescu" University
e-mail: adrian.bantas@gmail.com

**Faculty of Political Science, University of Bucharest
e-mail: sebastian.balanica@fspub.unibuc.ro

Abstract

In international relations, each state has historically pursued its own interests by various means. Although these have not always taken a violent form (for example, there are international actors such as the empires of successive Chinese dynasties which, in their relations with their neighbours, emphasized the respect for the emperor and prestige at the expense of violence, or the Ottoman Empire which, after its initial expansion phase, created a concentric system of peripheral actors with varying degrees of autonomy), before the signing of the UN Charter, the use of violence was not definitively forbidden between them either. More precisely, there are actors who, since then and as a result of successive changes in regimes and international orientations, have renounced the use of force or have severely limited it, making it at least predictable, and actors who, regardless of regime and context, adopt the same behaviour. In our view, Russia falls into the second category.

Keywords:
Russia; realism; use of violence; systemic aggressor; directions of expansion; threat perception; individual responsibility.

Introductory Considerations, Methodological Perspectives, and Conceptual Delimitations. Importance and utility of research

Whether we hold true the realism of Hans Morgenthau and his followers or see the world of international relations in the constructivist paradigm of Alexander Wendt[1], somewhat more optimistic and inclusive, Russia's aggressive behavior imposes itself as a reality that is almost impossible to contradict. The dilemma that is taking shape in these moments aims to characterize Russia's aggressive behavior in terms of international relations, as a dominant feature of Russian foreign policy throughout the history of Russian statehood, or as a conjectural feature of this policy, marked by the vision the regime led under President Vladimir Putin on international relations.

[1] Which presents us with a world where communities of international actors develop, borrow and, in a word, construct their own representation of international relations.

Solving this dilemma makes it necessary, in our opinion, to carry out a historical analysis of the behavior of the Russian state in international relations in order to identify its general paradigm, to see if the current dominant aggressiveness can be found throughout successive periods of the Russian state or whether it represents, rather, a characteristic trait of the post-1999 period, the beginning of Vladimir Putin's regime. Of course, our research starts from a series of conceptual premises, which we will detail in what follows.

The first of these is represented by the fact that, by looking at the history of international relations, we can distinguish a tendency to progressively diminish the use of armed forces and the threat of their usage, especially after the signing, in June 1945, of the Charter of the United Nations and the gradual establishment of a balance of nuclear powers, between the United States of America and the Union of Soviet Socialist Republics[2], characterized by mutually assured destruction (Ray 2022).

[2] State that ceased to exist on 26.12.1991, whose main successor, according to public international law, is the current Russian Federation.

Before these moments, war was considered a legitimate tool for pursuing the interests of states[3], for a plurality of conceptual, legal and practical reasons, being almost omnipresent in the history of mankind, on an area that coincided, in general terms, with the spread of human societies. Currently, according to specialized literature (Buzan 2017; Roberts and Westad 2018; Kissinger 2021) the latter represents the exception rather than the rule in terms of international relations, being concentrated within an area that surrounds the world map, but having a limited extent to the north and south of the Equator.

[3] This concept began to be attacked only with the signing of the Pact of the League of Nations (on 28.06.1919, during the Paris Peace Conference) and, more significantly, by the Briand-Kellogg Pact (on 27.08.1928, also in Paris).

The second premise, which derives from the first, implies that, although the vast majority, if not all states existing at this time, have either consistently

used armed aggression as a tool to pursue their own interests internationally, or are the successors of some states that have behaved this way throughout history, their behavior in international relations has undergone a progressive transition in a period whose beginning we previously identified as roughly coinciding with the end of the Second World War. These results of the major transformations undergone led to the current behavior, characterized predominantly by the non-use, or limited and localized use, of armed force, or the threat of the use of armed force, in relation to other members of the international community.

Another crucial premise is that, even if there are certain exceptional situations, of strict interpretation and application, in which international law considers that armed force can be used, its use only in these situations is sufficiently predictable for the entire international community that international actors acknowledge that, if they do not fall into these situations (for example, if they do not commit acts of genocide that could be the basis for the use of armed force), they will be held accountable. As a result, a state that uses armed force only in such cases cannot be considered a systemic aggressor because its actions are predictable and directed only against actors whose actions generate far more insecurity than armed intervention against them would. Conversely, the use of military force by systemic aggressors is not circumscribed by this condition, being directed against states whose interests diverge from its own, therefore making the use of force difficult to predict, which turns it into a threat to the security of states likely to represent the target of its aggressions.

Finally, the last of the premises from which our study debuts is that Vladimir Putin is, through the power associated with the presidential office of the Russian Federation and through his personal influence, the most representative person for the political and constitutional architecture of Russia, being of the highest degree in a position to influence the conduct of this state externally, compared to other politico-institutional actors in Russia. This fact, which has, in turn, become notorious, has been repeatedly demonstrated in specialized literature (Saari and Secrieru 2022), alongside the overall role of the Russian head of state over its whole history (Figes 2018), but it can also be ascertained through an analysis of the role of the President, as it is enshrined by the Constitution of the Russian Federation.

The importance of our study is conferred by the fact that, from an eventual conclusion that Russia represents a systemic aggressor, possible regime changes will not significantly influence its behavior. Conversely, if we find that Russia is not a systemic aggressor, but that its aggressive behavior is mainly caused by the decisions of President Vladimir Putin, regime changes, especially in the sense of democratizing the political and constitutional regime in the federation, could lead to changes in major scope in Russia's behavior in international relations.

Beyond the seemingly binary nature of this dilemma, the existence of an intermediate solution is not only possible but also, given the complexity of the causes of events in

international relations, quite probable. In this case, Russia would remain a systemic aggressor, but the individual contribution of the most representative person within each regime could accentuate or mitigate the tendencies generated by this character.

Such a conclusion could mean actively pursuing both the deterrence of Russia from using its military force in international relations and encouraging possible changes in the dominant characteristics of the power regime in Russia, including in the sense of closer cooperation with international courts in the direction of bringing to justice the persons guilty of generating and supporting wars of aggression or committing crimes against humanity, could lead to diminishing the threat from the actions of the Russian state.

To answer the research question of whether Russia is a systemic aggressor or not, and to open up new possibilities for research development related to using our findings to answer questions about how the threat of a systemically aggressive Russia can be managed, we will use the bibliographic research method and we will start from a historic analysis of Russia's aggressive tendencies. This analysis will be followed by the verification of the perpetuation of these trends in the present in order to, finally, analyze the role of President Vladimir Putin in the light of the command responsibility enshrined in public international law and to conclude by presenting the conclusions of the study in the light of the three possibilities exposed above.

Of course, the determination of the exact starting point of the contemporary period of Russian aggression may be subject to certain debates. However, in our opinion, it is reasonable to identify this moment with the beginning of support for separatist movements in the Russian-speaking East of Ukraine. We have opted for this view mainly because the occupation of the Crimean Peninsula, the other likely "candidate" for this "post", is rather an integral part of Russian aggression against Ukraine and one of its main objectives[4], and previous actions may easily be considered both as serving the goal of creating frozen conflict, and as part of a disinformation campaign that has induced both public opinion and decision-makers in Ukraine and throughout the Western world to believe in future Russian aggression on a large scale directed against Ukraine from an eastern direction, followed by the unexpected offensive directed against Crimea.

The Russian invasion of Georgia in 2008 can also be considered a defining moment, as the first Russian military aggression directed directly against a sovereign state after the breakup of the Soviet Union (although they also received military support from Russia: for example, the Transnistrian separatist forces in the war against the Republic of Moldova, or the Armenian forces in the conflict against Azerbaijan in Nagorno-Karabakh). But, in order

[4] Along with the creation and, subsequently, the maintenance of a frozen conflict that prevents (not so much theoretically-legally, as practically) Ukraine from acquiring the status of a member state of NATO and the EU.

to facilitate the transmission of the message of the article, we have opted for the fiction of separating the Russian-Georgian conflict from the Russian-Ukrainian one, assuming the fact that the two moments represent as many distinct stages as possible in Russia's international conduct after the breakup of the Soviet Union, even if the pattern and objectives are strikingly similar.

No matter how we look at things, the above also represents the most conclusive proof of the aggressive nature of the behavior of the Russian state in relations with other international actors. What we wish to further assert is, on one hand, the constancy of this aggressiveness and, on the other, the multiple, hybrid forms it currently takes.

1. Brief historical perspective on the expansion of the Russian state, from the reign of Tsar Ivan III (1452-1503 AD) to the present. How far is too far?

By making a short historical excursion, we can state with sufficient certainty that, from the beginning of Russian expansionism, which we can say overlaps, for the most part, with the reign of Tsar Ivan the Terrible, it followed several main directions.

1.1. The northern direction of expansion

One of them concerned the former Duchy of Novgorod, annihilated relatively quickly by the Duchy of Moscow, before the reign of the aforementioned Tsar. Throughout subsequent eras, such as that defined by the reign of Tsar Peter the Great and the Great Northern War, as well as throughout episodes not so dramatic, but by no means without consequences (such as the annexation of Finland in 1812), Russian expansion in this direction led, at its height, to the exercise of control over the Baltic States and Finland. In the contemporary era, the direction in question might seem if not abandoned, then secondary, but we will argue in due course the erroneous nature of this impression.

1.2. The Eastern and southern directions. The Caucasus Mountains, the southern sector of the Volga River, Central Asia and Siberia

In a random order[5], a second direction is represented by the expansion in the direction of the mouths of the Don and the Volga, of Central Asia and the Far East. In turn, the expansion in this direction can be said to have begun mainly during the reign of Tsar Ivan the Terrible, even if the entire period of coexistence between the Russian states following Kievan Rus and the successor states of the Mongol Empire presents a permanent alternation of conflict and collaboration. Like the first example, the direction in question led to the occupation of Central Asia (defined throughout the 19th century),

[5] Since neither a hierarchy nor a sufficiently precise chronology can be established between the directions we will list, they are often pursued simultaneously (of course, at different intensities), depending on the opportunities and imperatives of each historical moment.

the colonization of Siberia[6] and confrontations with China (for control over Mongolia and beyond), as well as with Japan (in main to the conflict that started in 1904).

A secondary direction emerged from this main one (not necessarily from the point of view of importance), represented by the expansion in the Caucasian region[7]. Following confrontations with states such as the Ottoman Empire, Persia, Georgia and more, which count episodes located in three distinct centuries, this direction led to the occupation of a territory that today would include, in the south of the Caucasus mountains, the states of Georgia, Armenia and Azerbaijan, but which included, at the height of the territorial expansion of the Russian Empire, a significant part of the Turkish region of Kars, for example.

1.3. The western direction. Expansion to the detriment of the Polish state

Yet another direction of expansion led to a confrontation between the Russian and Polish states in their various forms of existence. If the first confrontations between Russia and Poland[8] can be identified before this turning point, the defining moment of the Russian-Polish relationship can be said to have been represented by the occupation of Moscow by Poland, during those so-called "Troubled Times" that preceded the accession to the throne of the tsars of the Romanov dynasty. Why have we considered this moment as a turning point? Because, as stated in the specialized literature (D'Encausse 2015), the shock generated in Russian society by the occupation of Moscow irreversibly accentuated the cultural-historical theme of the vulnerability of the "open" borders of the Russian space and, as can be seen from a simple look at the relevant maps, they were not, with rare exceptions, delimited by natural relief elements, such as mountains, rivers, deserts, etc. For example, if Europe is furrowed almost from one end to the other by valleys of rivers and streams, often closed between high mountains, if the Chinese civilization evolved in a space bounded by the Gobi desert, by the mountain ranges of Central Asia (and in especially that of the Himalayas), by the jungles of Indochina and the Pacific Ocean, being open only to invasions from the Mongolian and Manchurian steppes, and if the United States of America occupies an area bordered by two oceans and very little exposed to land aggression, the Russian state has evolved into regions defined by relatively flat landforms, which can constitute an obstacle to possible invasions only by their vast extent and harsh climate. Of course, when the Russian state, in its expansion, encountered a "natural" boundary (represented by the Ural Mountains), it chose to go far beyond to the east and southeast.

Returning to the Russian expansion in the general direction of Poland, although this is not the place for an exhaustive enumeration of the episodes of Russian-Polish confrontation[9], we mention the fact that, following large-scale

[6] A colonization that we could, without too much fear of making a mistake, include in the directions of Russia's expansion, because, although it may present a less offensive character compared to the other examples, as a result of the absence of state formations in that territory and the presence in large uninhabited or sporadically inhabited geographical areas, the relations of the Russian settlers with the autochthonous populations took various forms from which conflict and coercion were never absent, being an almost natural corollary of trade relations.

[7] Since the first confrontations with the Ottoman Empire, placed in the 16th century and the later ones, with Persia, but the real development of this direction will occur only in the 18th century.

[8] We use these names to simplify the reading, since otherwise we should refer to entities such as the Grand Duchy of Moscow, the Russian Empire, the Union of Soviet Socialist Republics, etc., for Russia, and the Confederation (Rzeczpospolita Polska) or the Polish Republic, for Poland.

[9] In fact, one of the objectives of this article is to introduce themes that we intend to develop in the future issues of the journal.

military and diplomatic actions[10], spread over several centuries, the Russian state ended up occupying, at the height of its expansion, an extremely vast territory, which today would roughly correspond to part of the Baltic states, Belarus, the largest part of Ukraine, and almost all of contemporary Poland, including the capital of the Polish state, Warsaw, being, subsequently, forced to suppress, most of the time with extreme violence, the successive uprisings of the Polish freedom fighters (Davies 2014).

[10] See, in this sense, the three partitions of Poland between the Russian Empire, the Kingdom of Prussia and the Austrian Empire, which led to the demise of the Polish Confederation.

1.4. Southeast direction. The Russo-Ottoman Wars

We have left for last what is undoubtedly the most problematic direction of aggressive expansion of the Russian state, at least from our perspective. It is, as the reader has probably already guessed, the one we can call "southeast" (Buşe 2012). It is problematic because, it is a movement that had (missed) its debut in the confrontation between the Russian Empire, led by Tsar Peter the Great, and the Ottoman Empire. This ended with the Ottoman victory at Stănileşti in June 1770 and with a course favorable to the Russian Empire with the Russo-Turkish War of 1768 -1774[11], the latter ended up occupying a vast area, bordering the Black Sea and the mouths of the Danube, which today would include, roughly, the south of Ukraine, the Crimean Peninsula, and the entire territory of the historical province of Bessarabia (which, of course, is not limited to the territory of the Republic of Moldova today).

[11] Ended, among other things, with the secession of the Crimean Khanate from Ottoman suzerainty and its subsequent occupation by the Russian Empire under the ruling of Catherine the Great. Note how Russia currently invokes historical arguments for the annexation of Crimea, establishing itself where the invoked history begins to flow. In this logic, we do not see why possible territorial claims of Turkey on Crimea would not be more pertinent.

This direction presents, for us, a particular interest, both because of the fact that most of the confrontations between the Russian and Ottoman Empires took place in a theater of war that overlapped almost completely with the principalities of Moldavia and Wallachia, at that time under Ottoman suzerainty, as well as on account of the methods used by those responsible of Russian imperial propaganda and other subversive actions aimed at provoking disputes between the various communities in the Ottoman Empire and, thus, justifying Russian aggressions against the Ottoman state, presenting them as interventions intended to protect the communities allegedly injured.

2. Vladimir Putin as an independent factor of aggression

However, there is a certain idea that must be emphasized when we refer to the conflicts in which the Russian Federation has been involved. It is obvious, since Russia is under an authoritarian regime, that the involvement in a conflict, regardless of the situation, does not arise from the collective will of the nation, but from the singular will of its leader. In the present case, Vladimir Putin can be an independent factor of aggression. A brief look at the post-communist history of Russia may help paint this picture more clearly.

Starting with the year 1991, and implicitly with the mandate of Boris Yeltsin, the Russian Federation has been involved in numerous conflicts, but the long-lasting ones, as well as the most aggressive ones, were during the presidency of Vladimir Putin. In 1991, the first conflicts began, namely the Georgian Civil War, with the Zviadist revolt and the South Ossetian War. Note the Russian duality: if in the Georgian Civil War, Russia supported the Georgian government, in the South Ossetian War, the Russians supported the state of South Ossetia (Armstrong, Farrell and Maiguashca 2006).

The year 1992 marks the beginning of four new conflicts, namely: the War in Abkhazia, with Russia supporting Abkhazia; the Transnistria War, with Russia and elements of the former Soviet 14th Guards Army being among those directly involved in supporting Transnistrian independence. Also, in the same year, the East Prigorodny Conflict begins, with Russia supporting the Republic of North Ossetia-Alania against the Ingush militia; as well as the Tajikistani Civil War against the Islamist-Taliban factions and the Tajik opposition (Kemoklidze, et al. 2014; Rekawek 2017; Meijer and Wyss 2018). In 1994, Russia would once again begin to fight on multiple fronts, with the outbreak of the First Chechen War, which ended with a defeat in 1996, with the signing of the Khasav-Yurt Accord, being – until now – the only conflict lost by Moscow (Socher 2021).

In 1999, two interdependent conflicts will begin, namely the War of Dagestan, which will trigger, in the same year, the Second Chechen War. If the conflict in Dagestan ends in the same year, the one in Chechnya will continue until 2009. The same year, 1999, also marks the end of Yeltsin's mandate as, since 2000, the Russian Federation has had a new president in the person of Vladimir Putin (Brannon 2016). A year before the end of the second conflict in Chechnya, in 2008, the Russian Federation would start the Russo-Georgian War, through which it occupied the republics of Abkhazia and South Ossetia. In 2009, the Insurgency in the North Caucasus would begin, with the Russian Federation, Chechnya, Dagestan, Ingushetia, North Ossetia-Alania and Kabardino-Balkaria fighting against the so-called Islamic Emirate of the Caucasus, a conflict that will last until 2017, ending with the defeat of the Islamists (Schaefer 2010). The year 2014 would mark the Russian annexation of Crimea and would be the precursor of the invasion of Ukraine in 2022. The Russian Federation would also get involved in the conflict in Syria, starting in 2015, supporting the government of Bashar al-Assad, on the same side as Iran and Hezbollah. Last but not least, the Russian Federation is actively involved in the Central African Republic (CAR) Civil War, since 2018, supporting the CAR in the fight against the rebels of the Coalition of Patriots for Change (Slider and Wegren 2022).

From the above, some at least interesting conclusions emerge, namely: even if Russia had several conflicts during the Yeltsin period, they had a much shorter duration. By comparison, the conflicts during Putin's mandates, including those in tandem with Medvedev, were either significantly longer, or have not yet ended. All these things

have a common denominator in the person of Vladimir Putin, and an expansionist policy based on a pan-Slavist type of nationalism, which shows the fact that, at the level of mentality, it was not possible to overcome the moment of the disintegration of the Soviet Union. The continuous and unjustified aggression of a country that seems to be desperately looking for new conflicts is nothing more than the result of an authoritarian policy that wants to restore a status quo from before the 90s (Đorđević, et al. 2023).

2.1. Putin: an independent factor of aggression in the international law paradigm

It is also important to show why the substantiation of the fact that Putin is an independent factor of aggression can be found not only in the area of geopolitics and international relations, but also in the area of international law. Thus, in the international criminal system, implicitly in international law, command responsibility is a mode of criminal liability aimed at the individual and not the state or organizational actor. Command responsibility is based on the idea that an individual in a position of authority who fails to prevent a criminal act is responsible for doing so. Moreover, this fundamental idea, applying a causal chain will result – in a situational framework – in two consequences that support this paradigm.

The first consequence is that command responsibility, and therefore failure from an authoritative point of view – most of the time at the military level, being the most common case – constitutes a deviation from the military codes, implicitly the laws that govern these sectors.

The second consequence, with an automatic character, is that in case of a failure of authority, implicitly the activation of command responsibility, the individual becomes an accomplice of his subordinates who committed the criminal acts (Stahn 2021, 158-160).

Many discussions were held on the two consequences, of a dualistic type, featuring opinions that supported the change in the framing of command responsibility either in the area of omission or in the participative area – to be determined, on a case-by-case basis, the voluntary or involuntary character – or in the area of general criminal liability, as having a common law character (Sliedregt 2012; Klabbers 2021). But, considering the theoretical framework in which criminal liability is placed – of course, one can argue in favor of the syncretism between elements related to omission or indirect liability – the justification according to which the individual in the area of authority – on the hierarchical scale – is directly responsible for the acts of his subordinates if they are the result of culpability of the obligations of (Stahn 2021, 159-160; Browers 2012; Darcy 2007).

The application framework of the command responsibility had to be built precisely in order to be able, on the one hand, to acquire the adaptability necessary for the transfer of context – from the military to the civilian one, and vice versa – and, on the other hand, to avoid the appearance of lacunae or ambiguous areas due to too

broad a meaning that command responsibility could have had. It had to be explained and argued that command responsibility does not mean, given its indirect nature, that the individual in the hierarchical position will suffer the same set of consequences or will have the same degree of responsibility as his subordinates. The proportionality of individual liability will be related to the seriousness of the facts and acts committed by his subordinates (Othman 2005, 253-270; Ghanayim and Shany 2021).

This is the area where certain differences between command responsibility and its applicability in the military versus the civilian setting appear for the first time. If in the military context, things are quite clear, there are still some possibilities of interpretation in the civilian context. Thus, command responsibility being extended to civilians – precisely because of the fluidity of international law and the multitude of situations, or cases encountered – was attached to the concept of authority, be it military or civilian. The argument in favor of this expansion was, in addition to that of fluidity, that the degree of control that a civil authority exercises – at an organizational or societal level – can be counterbalanced – of course, in certain situations such as conflict – with military authority. It also provides an answer to questions about the authority and ability that a civil authority has – and can use – for both prevention and punishment and regulation of potential criminal acts and deeds committed by subordinates (Stahn 2021, 141-142).

In addition to these, there is a relevant case for this discussion, pending before the ICJ, namely *Ukraine v. Russian Federation (2017)*[12]. Thus, for this case, arguments were brought according to which the ICJ could apply command responsibility. One idea brought to the table was that, depending on the framing that was to be applied to the conflict, namely either international armed conflict or non-international armed conflict, command responsibility could be applicable at a dualistic level. If the conflict was framed as non-international, then commanders of separatist groups and movements, who were culpable under both Ukrainian and international law, could be held individually, and under command responsibility, responsible. If the conflict was characterized as international, then including the commanders from the side of the Russian Federation were guilty according to the Geneva Conventions (Medvedieva and Korotkyi 2021, 60-65). Therefore, if it is proven – both in the case of the separatist commanders and in the case of the Russian ones – that there was an intention to attack – direct responsibility – and/or knowledge of the imminence of an attack, of the potential damage that would be caused, etc. – indirect responsibility, *ergo* command responsibility – they could be assigned a dual degree of culpability. Thus, the ICJ could invoke command responsibility both for the Ukrainian separatists and for the Russian commanders, something that, up to the current stage of the case, has not yet been applied, collective responsibility being preferred, implicitly the

[12] Application of the International Convention for the Suppression of the Financing of Terrorism and of the International Convention on the Elimination of All Forms of Racial Discrimination.

state one (Klabbers 2021; Medvedieva and Korotkyi 2021, 63-65). Therefore, there are premises, at the level of international law, based on which Vladimir Putin could be seen as an independent factor of aggression.

3. What about today? Is Russia still aggressive?

From a practical point of view, the above description is useful if we can determine a connection, some kind of continuity between Russia's actions in the historical past, within each direction of expansion, and Russia's foreign policy today. In other words, the question that arises at this moment is the following: is Russia still aggressive today? Analyzing the main foreign actions of Russia, in the mentioned directions, from the breakup of the Soviet Union until today, the conclusion we reach almost inevitably is that Russia continues to present itself as an aggressive international actor, in almost the same directions that it has followed since the beginning of its expansion. Although we only wish to present this aspect briefly, a simple analysis of Russia's actions during this period demonstrates the correctness of this statement. Let us therefore analyze the situation of the expansion directions in the order of their presentation.

Thus, as far as the Baltic direction is concerned, the moments when Soviet or Russian submarines penetrated the territorial waters of Sweden are well known, along with many other incidents or elements of diplomatic tension that can be identified with a simple search on the Internet. The same goes with regard to the Baltic States; the tensions and incidents between them and Russia need no introduction, as the 2007 cyber-attack against Estonia that crippled much of that state's government cyber infrastructure is perhaps the most representative example, but by no means the only one. The membership of the Baltic States in NATO represents, however, a sufficient element of deterring some "traditional" offensive actions carried out by Russia, but this does not even remotely exclude the existence, in the future, of elements of a hybrid confrontation, following the model of the cyber-attack mentioned above.

Nor can the eastern direction, towards Central Asia and the Far East, be considered abandoned. If the actual territorial expansion towards the Far East became anachronistic with the consolidation of the Chinese state, after the Second World War, the interests of Russia and China in terms of the exploitation of underground resources in the Siberian area cannot be considered nearly as harmonized as the parties would like to consider them. And, as far as Central Asia is concerned, the interests of Russia and China regarding the markets of the states in the region, the infrastructure projects that China wants done and can be considered not only disharmonized, but quite the opposite. And, if we add to these the ambitions of Turkey or Iran, the result is a picture in which Russia must exert ever greater pressure to try to prevent the ex-Soviet states in the Central Asian region from detaching more and more from on the political-economic orbit of the former imperial power (Popescu and Makocki 2017).

Of course, the branch off of this, the Caucasian one, is as current as ever, even if it takes different forms. Related to Russia's involvement in the conflict between Armenia and Azerbaijan, since the end of the Soviet era, enough specialized works have been written that there is no need to revisit the subject in detail; about Russia's involvement in supporting the separatist republics of Abkhazia and South Ossetia, in Georgia, likewise. The Russian invasion of Georgia, in 2008, is basically the moment that brought the aggressive policy of post-Soviet Russia back to the world's attention. More recently, the stationing of Russian forces in Karabakh, the support given to Armenia in the conflict with Azerbaijan (conditional on the abandonment of negotiations with the European Union and accession to the Eurasian Economic Community), along with the deployment of Russian troops, as peacekeeping forces, in the portion of territory remaining under Armenian control after the recent successful Azeri offensive supported by Turkey, through which Azerbaijan managed to recover most of Karabakh under Armenian occupation, is as much evidence of Russia's continued aggressive involvement in the politics of the states south of the Caucasian mountain range.

The western direction of expansion is, however, perhaps the most obvious for us and not only, since 2013. The episodes of confrontation between the pro-Russian separatists in Ukraine, the frequent threats of armed invasion, the occupation of Crimea, Russia's participation in the Minsk format, in support of the claims of the separatists in the Don basin and the other political-economic actions directed against Ukraine (such as the interruption of the natural gas supply or the threat with this measure) has been occupying the public agenda of Romania, Europe and the United States for over seven years. Therefore, we consider that the persistence of Russian aggression in this direction of expansion is self-evident, an obvious fact whose demonstration in this study risks becoming redundant (Bantaș and Dumitru 2018, 25-47). Similarly, the influence exerted by Russia on its neighboring state, Belarus, which borders on total control, by supporting the Lukashenko regime is, in turn, on record.

We have left, for the end, the southwestern direction of expansion, the one that interests us, perhaps, the most. Of course, it would be easy to say that, apart from supporting the Transnistrian separatist entity, actions with territorial consequences by Russia in this geographical region can be considered anachronistic. But such a conclusion remains valid only as long as Russia or the entities controlled by it do not directly border the territory of the Republic of Moldova (in which we also include the Transnistrian separatist entity). If, through new actions directed against the state integrity of Ukraine, a direct territorial link would be created between Transnistria and Russia, this conclusion could undergo important adjustments.

In addition, nowadays, the conduct of an aggressive policy no longer requires predominantly military means. Campaigns supported by disinformation can be of a similar nature, for example, aimed at instilling civil disobedience, weakening

the cohesion of a society, making it vulnerable to threats of a sanitary nature; or weakening the sense of belonging and popular support for maintaining NATO and EU membership, i.e. exactly those obstacles that, at the moment, stand in the way of direct aggressions by Russia. However, this subject is to be addressed extensively in our future efforts.

Thus, the only possible conclusion is that Russia is still as aggressive today as ever, from Ivan the Terrible through the age of Peter the Great, along the same lines. How can such aggression be stopped? As in the past, through a common and firm resistance of the entire Western world, centered on "*the values common to the European Union, in general, and to each democratic state in particular, as the foundation of economic and social progress and the growth [welfare] of their members*" (Marinescu 2020, 46). How can this resistance be organized and carried out? Well, as already stated above, this study only establishes the framework on the basis of which the articles that will follow will be developed, and the theme of resistance to Russia's aggressive actions will not be missing from them.

The solution to the threats generated by this character remains, in our view, the promotion of a rules-based international order. Of course, the implementation of an international order based on norms, which debuted with the adoption of the United Nations Charter, is an arduous and still unfinished endeavor, and any such approach will be *achieved gradually, (in line) with the economic and political evolution at national and international level* (Salomia and Mihalache 2016, 166); however, once this objective is achieved, we anticipate the production of what could be characterized as a spill-over effect of integration, from regional initiatives such as the European Union, based on *"ties that go beyond the framework of the nation-state (...), voluntary adhesion (...), peaceful transformation"* (Dumitrașcu 2006, 74).

Conclusions. In the end, what kind of aggressor is Russia?

In the light of what has been presented throughout this study, we believe that Russia's aggression, like so many other events specific to international relations and life in general, is likely to be associated with a set of causes and characterized by a plurality of features. By the constancy and even by the predictability of its acts of aggression, Russia can be considered a systemic aggressor, a fact demonstrated by the historical analysis carried out. In fact, the permanence of its aggressive behavior is so striking that almost every ruler of the Russian state, from Ivan III to the present day, has been involved in at least one aggressive action externally or internally, including the civil war of Chechnya. Considering the fact that the analyzed period spans almost six centuries, such constancy, such unswerving pursuit of the same general objectives, through the same violent means, represents a performance unmatched by any other contemporary state and comparable, perhaps, with the existence of the great empires of Antiquity.

And yet, the course of history is not inevitable, and the actions of decision-makers, even if they are often severely limited by circumstances, are almost always able to influence, if not their course, at least the overall framework. As we have shown using the comparative examples of the Yeltsin and Putin mandates, the level of aggression is neither inevitable nor constant. Moreover, the inclusion in the research of the mandate of former president Mikhail Gorbachev is likely to demonstrate additionally that the actions of decision-makers can significantly influence the course of events. But, through its exceptional character, it only confirms the rule, and this is, in our opinion, represented by the systemic nature of the aggressiveness of the Russian state.

References

Armstrong, David, Theo Farrell, and Bice Maiguashca. 2006. *Force and Legitimacy in World Politics.* Cambridge University Press.

Bantaș, Dragoș-Adrian, and George-Dorinel Dumitru. 2018. „Conflicte înghețate în Regiunea Caucazului. Cauze, Desfășurare Și Perspective." *LEX: Revista consilierilor juridici din armată,* nr. 2.

Brannon, Robert. 2016. *Russian Civil-Military Relations.* Routledge.

Browers, M.P.W. 2012. *The Law of Command Responsibility.* Wolf Legal Publishers.

Bușe, Dorel. 2012. *Geopolitica Rusiei la Dunăre și Marea Neagră în perioada 1812-1878.* București: Editura Universității Naţionale de Apărare „Carol I".

Buzan, Barry. 2017. *Popoarele, statele și frica. O agendă pentru studii de securitate internațională în epoca de după Războiul Rece.* Chișinău: Editura Cartier.

Darcy, Shane. 2007. *Collective Responsibility and Accountability under International Law.* Transnational Publishers.

Davies, Norman. 2014. *Istoria Poloniei. Terenul De Joacă a Lui Dumnezeu (Volumul I: De la origini până La 1795; Volumul II: De la 1795 până în prezent).* Bucureşti: Editura Polirom.

D'Encausse, Hélène Carrère. 2015. *Orgoliile Kremlinului. O istorie a Imperiului Rus de la 1552 până astăzi.* Bucureşti: Editura Orizonturi.

Đorđević, Vladimir, Mikhail Suslov, Marek Čejka, Ondřej Mocek, and Martin Hrabálek. 2023. "Revisiting Pan-Slavism in the Contemporary Perspective." 51 (1): 3-13. https://doi.org/https://doi.org/10.1017/nps.2022.75.

Dumitrașcu, Mihaela-Augustina. 2006. *Evoluția Comunităților Europene de la integrare economică la integrare politică – implicații asupra ordinii juridice comunitare.* București: Editura C. H. Beck.

Figes, Orlando. 2018. *Dansul Natașei. O istorie culturală a Rusiei.* Bucureşti: Editura Polirom.

Ghanayim, Khalid, and Yuval Shany. 2021. *The Quest for Core Values in the Application of Legal Norms Essays in Honor of Mordechai Kremnitzer.* Springer.

Howard, Douglas A. 2021. *O Istorie a Imperiului Otoman.* București: Editura Polirom.

International Court of Justice. 2021. *Application of the International Convention for the Suppression of the Financing of Terrorism and of the International Convention on the Elimination of All Forms of Racial Discrimination.* https://www.icj-cij.org/case/166.

Kemoklidze, Nino, Cerwin Moore, Jeremy Smith, and Gallina Yemelianova. 2014. *Many Faces of the Caucasus.* Routledge, Taylor & Francis Group.

Kissinger, Henry. 2021. *Ordinea mondială.* București: Editura RAO.

Klabbers, Jan. 2021. *International Law.* 3rd edition. Cambridge University Press.

Marinescu, Delia-Mihaela. 2020. "Proceedings of the «Romania in the New International Security Environment»." București: Editura Universității Naționale de Apărare „Carol I".

Medvedieva, M.O., and T.R. Korotkyi. 2021. "Responsibility for The Environmental Damage Caused During The Armed Conflict Between Ukraine And The Russian Federation: Opportunities In The Algorithm Of Protecting National Interests." *Actual Problems of International Relations,* no. 139. https://doi.org/10.17721/apmv.2019.139.0.58-67.

Meijer, Hugo, and Marco Wyss. 2018. *The Handbook of European Defense Policies and Armed Forces.* Oxford University Press.

Othman, Mohamed C. 2005. *Accountability for International Humanitarian Law Violations the Case of Rwanda and East Timor.* Springer.

Popescu, Nicu, and Michal Makocki. 2017. "China and Russia: An Eastern Partnership in the Making?" https://www.iss.europa.eu/content/china-and-russia-eastern-partnership-making.

Putin, Vladimir Vladimirovich. 2022. "Address by the President of the Russian Federation." http://en.kremlin.ru/events/president/news/67843.

—. 2021. "On the Historical Unity of Russians and Ukrainians." http://en.kremlin.ru/events/president/news/66181.

Ray, Michael. 2022. "Mutual Assured Destruction." În *Encyclopaedia Britannica*, editor Adam Augustyn și Gloria Lotha. https://www.britannica.com/topic/mutual-assured-destruction.

Rekawek, Kacper. 2017. *Not Only Syria? The Phenomenon of Foreign Fighters in a Comparative Perspective.* IOS Press.

Roberts, J.M., and Odd Arne Westad. 2018. *Istoria lumii. Din preistorie până în prezent.* București: Editura Polirom.

Saari, Sinikukka, and Stanislav Secrieru. 2022. "Russian Futures 2030: The Shape of Things to Come." https://www.iss.europa.eu/content/russian-futures-2030.

Salomia, Oana Mihaela, and Augustin Mihalache. 2016. „Principiul egalității statelor membre în cadrul Uniunii Europene ." *Dreptul,* nr. 1: 166-174.

Schaefer, Robert W. 2010. *The Insurgency in Chechnya and the North Caucasus: From Gazavat to Jihad.* Praeger Security International.

Slider, Darrell, and Stephen K. Wegren. 2022. *Putin's Russia.* 8th ed. Rowman&Littlefield.

Sliedregt, Elies Van. 2012. *Individual Criminal Responsibility in International Law.* Oxford University Press.

Socher, Johannes. 2021. *Russia and the Right to Self-Determination in the Post-Soviet Space.* Oxford University Press.

Stahn, Carsten. 2021. *A Critical Introduction to International Criminal Law.* Cambridge University Press.

No.2/2023, APRIL-JUNE
https://doi.org/10.53477/2284-9378-23-24

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Leadership, competitive intelligence and Robert Oppenheimer's pivotal role in the dawn of the nuclear age

Rodica-Cristina BĂLAN-LISEANU, Ph.D.*

*Ministry of Education of Romania
e-mail: rodica.liseanu@yahoo.com

Abstract

In an era of globalization, innovation, and competitive intelligence, the nuclear supply chain is continually evolving and increasing its capabilities. The top-secret operation ALSOS plays a key role in the (re)evolution of atomic energy as the energy of the future, with a constant focus on the responsible use of atomic energy. The US, a nuclear hegemon, has harnessed its leaders to their full potential, with J. Robert Oppenheimer being one of the leading names in charismatic, competitive, and transformational leadership. Through qualitative and content analysis, this article proposes a reflection on the origins and evolution of change in the nuclear field, in a continuous struggle for supremacy, connecting with current desiderata in the sphere of innovation, built on different leadership styles. The interest in leadership is recurrent, and the model of Operation ALSOS, in line with the iconic figure of J. Robert Oppenheimer, is representative of motivating the harnessing of new promises to inspire and revolutionize the world.

Keywords:
atomic energy; competitive intelligence; leadership; Operation ALSOS; elite power; Robert Oppenheimer.

Competitive intelligence in the nuclear energy sphere is founded and structured on two types: strategic intelligence and tactical intelligence, each of which delineates different operational horizons. While the former is aimed at medium and long-term exploitation, the latter is aimed at immediate, short-term developments. *Knowledge Management* is about creating, analysing and processing knowledge and is part of the Strategic Intelligence Triad (Smith 2020) together with *Business Intelligence* and *Competitive Intelligence*, three fundamental elements in using knowledge to create and maintain a competitive advantage for personal benefit.

Humanity seems to have been guided by the adage attributed to the English philosopher Francis Bacon – "*Scientia potentia est*" (*Knowledge is power*), first found in the *Leviathan* by his secretary Thomas Hobbes. The United States of America, which has always held nuclear supremacy, was the world's only nuclear power between 1945 and 1949; it seems to have been guided by this aphorism, which was later elaborated by the American philosopher and essayist Ralph Waldo Emerson.

In an era of globalization, where dependence on fossil fuels is becoming unsustainable, there is increasing discussion of a renaissance built on reinvestment in the field and, consequently, the nuclear industry is experiencing growing competitiveness. Nuclear energy is thus emerging as the energy of the future, encompassing economic, military, and environmental considerations. Notably, the European Commission has classified it as green energy within the context of combating carbon dioxide emissions, which are the primary contributor to the greenhouse effect.

1. The evolution of the atomic weapon, from simple to complex

In his ongoing quest to rule the world, man has delved into the mysteries of the universe and sought answers to its most pressing questions. In his accelerated study of matter, the horizons of his thought have broadened, and paradoxes have been transformed into logical, proven, argued content. From the primary research lines of matter through physics and chemistry, specialists have set out to conduct advanced studies on the exploitation of the energy and nuclear fields. Thus, at the centre of its interests have been processes concerning nuclear energy, nuclear technologies, and nuclear safety, with regulations and legislation in force. In the nuclear age, competitive intelligence refers to the early identification of potential threats, but also to the identification of opportunities, in the processes of intelligence gathering, analysis and interpretation. This includes programmes to monitor nuclear programmes, identify and assess intent and capabilities, and security policies to promote balance and nuclear non-proliferation.

The 1970 Non-Proliferation Treaty (NPT) and other international agreements such as the Comprehensive Test Ban Treaty (CTBT) are designed to promote

disarmament, deterring the spread of nuclear weapons around the world, gradually leading to their complete elimination. In the arms race in 2023, there are states such as the USA, the Russian Federation, the United Kingdom, France and China, which are officially recognised by the Treaty as possessing nuclear weapons, and states not officially recognised by the NPT, such as India and Pakistan. Israel and North Korea are suspected of having nuclear capabilities but do not officially recognise their nuclear arsenal.

In 2023, nuclear states officially possess, according to statistics, around 12,500 operational nuclear weapons, their motivations for arming being deterrence and national security, regional interests and protection of allies, strategic autonomy, the balance of power, and prestige of status in international politics. Given the increased level of insecurity and tensions, nuclear proliferation can weaken diplomatic relations and diminish trust between states.

In a past-present pendulum swing, whereas in the 19th century, concern for the development of the nuclear breakthrough segment was feverish, today, at least at the level of official discourse, it is precisely disarmament and non-proliferation of weapons of mass destruction that are encouraged.

1.1. Brief history

Although in the 5th century BC the ancient Greeks claimed that the atom was indivisible, etymologically speaking the word *atomus* itself, first used by Democritus of Abdera translates in the same way, later, after almost 2000 years, research revealed its ability to split. The theoretical construction of the atom is based on Antoine Lavoisier's 1789 *Law of Conservation of Mass* (the mass of a closed system remains constant regardless of the processes within it), Joseph Proust's 1799 *Law of Definite Proportions* (substances have a well-determined qualitative and quantitative composition), and John Dalton's 1803 *Law of Multiple Proportions* (compound substances are formed when different elements interact in different reaction systems). (Iosif 2009)

In 1808, the English physicist and chemist John Dalton assigned atomic masses (a revolutionary concept at the time) to 20 known chemical elements, which he put together in a rudimentary table.

In 1869, based on his precursor's innovation, the Russian chemist Dimitri Mendeleev published the first globally recognised periodic table of elements, which included all 63 chemical elements known at that time, according to their atomic number. On the left-hand side were the metals and on the right the non-metals. A visionary, Mendeleev left spaces in his table for unknown chemical elements, accurately predicting their properties. In the last decade of the 19th century, scientific discoveries gradually evolved from explaining the phenomenon of radioactivity to the modern development of atomic energy.

In 1897, physicist J.J. Thomson was to discover the electron, with the idea of splitting the atom into electrons, protons and neutrons coming later. This negated the preliminary theory of the atom as the smallest particle.

The existence of the atom was proved in 1905 by Max Planck and Albert Einstein, through the accuracy of mathematical calculations. In addition, the research of Pierre and Marie Curie and their descendants Frédéric Joliot Curie and Irène Curie into radioactivity and the nucleus was recognised by Nobel Prizes in physics and chemistry. The extended Curie family has won a total of 5 such prizes. (Marcovici 2018, 29-30) Related to the famous prizes, Alfred Nobel's name is associated with the same area of research, the Swedish chemist and industrialist being the inventor of dynamite.

Radioactivity was discovered by the French physicist Henri Becquerel by chance, "*while studying uranium and the phosphorescence of uranium salts*" (Marcovici 2018, 29). In 1895, German physicist Wilhelm Roentgen observed that radiation emission penetrates opaque objects producing fluorescence, and his discovery prompted Becquerel to test fluorescent uranium salts. In 1896, he demonstrated that uranium is radioactive, that is, it emits penetrating radiation that would ionize gas (Jones 1985, 25). Although it is a thousand times more common than gold, uranium is considered a rare element.

The study of the structure of the atom built the scientific foundations of nuclear physics, pioneered by the New Zealand-born Englishman Ernest Rutherford. Discoveries such as the nuclear fission of the German Otto Hahn and his collaborators in 1938 followed, as the means to the most destructive of human inventions - the atomic weapon. Nuclear fission involves radioactive decay, splitting the nuclei of uranium atoms and discharging the energy inside. At the other end of the spectrum, nuclear fusion involves the union of several atomic particles to form a heavier nucleus.

Fission bombs, also called atomic or nuclear bombs, were tested in 1945, and hydrogen bombs, fusion-based bombs (also called thermonuclear) were tested in 1952. The destructive force of the hydrogen bomb is much greater than that of the atomic bomb. Given the similarity between the first Soviet bomb and the so-called *Little Boy* bomb dropped on Hiroshima four years earlier, the supremacy of the US as the sole nuclear power from 1945-1949 is confirmed. Also, after the Second World War, accelerators and particle detectors appeared, making it possible to study the effects of moving atoms at high energies.

1.2. Key personalities

The early nuclear age embodies aspects of competitive intelligence, with several names that became household names marking the period of bold experiments that would change the course of the world and history. Of these, the most resonant,

J. (Julius) Robert Oppenheimer (1904-1967) was even the inspiration for director Christopher Nolan's eponymous historical-biographical film creation to be released in July 2023. Oppenheimer was known as the father of the first atomic bomb - the A-bomb, following the resounding success of the Trinity Test, a controlled nuclear explosion carried out in the Los Alamos desert in the US state of New Mexico. The Trinity Nuclear Test (T.N.T.) was the code name for the world's first nuclear explosion on 16 July 1945. Without his initiative to bring scientists and physicists together in a remote and secret location, the atomic bomb would have been unattainable. He was the director and scientific leader of the giant Manhattan Atomic Project, and following the dropping of the two bombs on Japan, his image acquired an undesirable celebrity. *Little Boy,* the bomb dropped on 6 August 1945 on Hiroshima, was uranium-based, while *Fat Man*, the second bomb dropped three days later on Nagasaki, was plutonium-based.

In contrast to Oppenheimer's popularity, **Edward Teller** was a staunch anti-communist, far-right anti-liberal, known as the leader of the first Ivy Mike hydrogen bomb, a project approved by President Harry Truman in 1950. Thanks to this responsibility, he was nicknamed the father of the hydrogen bomb (the H-bomb). In 1946 he was decorated by President Harry Truman, and in 1963 he was given the Enrico Fermi Award by President John Kennedy. In 1957, he was also awarded the Légion d'Honneur in France, and in 1962 in Great Britain as a Foreign Fellow of the Royal Society of Great Britain. In order to persuade Oppenheimer to leave Alamos for good, he was to strike precisely at his sympathy for the Communists.

Leslie Groves is also among the iconic personalities, having built the world's first de facto atomic bomb, fulfilling his mission of commitment with the successful Trinity Test. He was the general appointed to head the top-secret Manhattan Atomic Project by US Secretary of War Henry L. Stimson, with the approval of President Franklin Delano Roosevelt.

It is important to note that, in support of subsequent events (Trinity Test, bombs dropped in Japan), President Roosevelt authorised the Manhattan Project on 28 December 1942 (Gosling 2010, 20). Leslie Groves became well known in the military world thanks to his management and engineering skills, and the project brought him international fame and recognition. Following the bombing of the Japanese cities of Hiroshima and Nagasaki, he was to be awarded the Legion of Merit Medal and the Service Medal by the US government (and later by the governments of Belgium, Britain and Nicaragua) and retroactively promoted to the rank of lieutenant general.

At the same time, the German anti-fascist physicist Klaus Fuchs, actively involved in the atomic bomb project, was, despite his professionalism, also the spy who allowed the information to be leaked. With assurances of loyalty from the British services, he was co-opted by the US into the top-secret Manhattan Project in 1943, and a year later was given unrestricted access to the top-security sector. Despite all the

security efforts of General Leslie Groves and Colonel Boris Pash, head of espionage and counter-espionage at Los Alamos, it was only in 1950 that his Soviet espionage status was discovered and he was convicted. After the war, he returned to England as a British nuclear worker, and his knowledge remains of great impact. Like Oppenheimer, Fuchs had affinities with the communist movement.

2. The Top-secret ALSOS Operation

The Manhattan Project, a unique American atomic program conducted from 1939-1946, was the secret pinnacle of the US military's participation in World War II. It was the effort that produced the atomic bombs that were instrumental in ending the war with Japan and also marked the beginning of a new era – the nuclear age. The creation of an atomic bomb was the result of effective collaboration between science, industry/engineering and the US military.

The Manhattan Project is highly complex, combining military and civilian aspects. The project is led by two brilliant professional profiles. On the one hand, the US government has appointed General Leslie Groves as Project Director and, on the other, it has appointed Robert Oppenheimer, a professor of physics at the University of California, Berkley, as Scientific Director of the Los Alamos programme. At the time of the recruitment, they were looking for a man of outstanding ability and hard work.

Colonel Boris Pash, a specialist counterintelligence officer, is tasked with vetting everyone involved in the top-secret Manhattan atomic project, including Oppenheimer. Although he relied on his loyalty and trusted that he was not a spy, he still recommended surveillance of him to acquaintances, knowing that his wife, brother and sister-in-law were Communists and that he had donated money to the Communist Party without even being a party member.

In early 1942, the American war leadership understood with certainty that the Allied forces were in a race with Germany for primacy in the development of an atomic weapon, and it was the Army that would be given the task of administering the atomic system. Moreover, only the army could provide security, military services, and liaison services, in the context in which the success of this program was imperative. Drawing on its experience and human resources, the Army created a new organisation made up of engineers – the Manhattan District. This was the embodiment of the extreme motivation of the US to hold the primacy of atomic weapons production in the arms race against Nazi Germany.

On July 1st, 1944, the District received AA-1 authority, the minimum required for procurement. In the summer of 1942, University of California physicist Robert Oppenheimer was directing the theoretical design and construction aspects of the atomic bomb. He proposed setting up a separate laboratory devoted exclusively to

such work, a proposal soon accepted by General Groves. Unique in history is the large number of genius scientists gathered in one place. Groves and Oppenheimer agreed that the region around Albuquerque, New Mexico seemed the most promising for this purpose. They chose an uninhabited, isolated area on a high plateau on the site of a former private boys' school – *Los Alamos Ranch School*, which included 54 buildings. During World War II, it was bought and turned into a secret nuclear research campus. Isolation was a strong argument in choosing the site, the nearest town being 16 miles away (almost 26 kilometres) (Jones 1985, 80-85).

The ALSOS Project in Manhattan's Engineer District was less well known, the ALSOS missions being an integral part of it. It encompasses scientific intelligence missions that took place in Europe in Italy, France and Germany (Atomic Heritage Foundation 2014). More specifically, it is an intelligence-gathering effort aimed at finding out how close Germany was to developing its own atomic weapon.

The mission codenames were deliberately chosen to be harmless, and unobtrusive, but the codename *ALSOS*, the Greek word for *grove*, seemed to attract undue attention, which annoyed the Manhattan Project team commander, General Leslie Groves. Under his command, elite German scientists, nuclear raw materials, research documents on the development of atomic energy, and uranium ore deposits were captured in various operations (Jones 1985, 281). The concept of the power elite developed by C. Wright Mills in his 1956 paper of the same name (Marshall and Scott 2014, 237) is reflected in this fervent search for those representatives with superior power operating in the segments of interest in the project. The Los Alamos elite was that minority destined to dominate the world, and the set of values by which they were guided gave them legitimacy.

3. Robert Oppenheimer – manager, leader and central architect of the atomic bomb

Since the earliest times, in their evolutionary process, people have alternated between different social capacities, so that some have chosen to listen more, others to be more influential in their way of making themselves heard, but all have shared different needs, interests, aspirations and motivations and have tried to influence each other. Thus, leaders influence their subordinates, and subordinates in turn influence the leaders' manifestations and behaviours. Dominant personalities can assert themselves by alternating between force and threats, or they can gain respect through credibility, competence and the consistency of personal example.

In a world dominated by unpredictability, uncertainty and disorder, today's major national and international challenges require military leaders and others to adopt new leadership measures with a focus on motivation and engagement.

3.1. Management and leadership in military operations

If an organisational chart clarifies the roles and functions of an organisation, in the context of crises, armed aggression, economic crises or pandemics, there is a need for a leader who can demonstrate effective authority both horizontally and vertically within an organisation or institution. Robert Oppenheimer was more than a manager, he was a leader and an inspirational role model. On the one hand, management is *"the process of directing, controlling and coordinating the activities of an organization/institution, together with the people who perform these functions."* (Duțu 2008, 25)

According to the Dictionary of Sociology, *"as a process, it is conventionally divided into general management of the organization's main objectives and personnel or specialized management that deals with support roles such as personnel, legal issues or research and development."* (Marshall and Scott 2014, 426) Applied to the military, it can be defined as *"the set of principles, functions, methods, and techniques used by commanders to accomplish missions assigned to a particular structure with minimal loss of human and material resources."* (Duțu 2008, 26) On the other hand, *leadership* is the ability of a leader to direct and lead a group beyond limits, assuming the integration and resolution of difficulties as part of the experience. The qualities of a leader are assertiveness, self-confidence, empathy, modesty, kindness, which build the status of a strong leader, able to direct, guide and protect his team (Chrétien 2020).

3.2. Leadership theories, according to historical criteria, can be classified into *personological theories, behaviourist theories, contingency theories, new leadership theories and situational theories* (Duțu 2008, 14-16).

a) Personological theories subsume charismatic leadership theory and trait theory (the late 1940s);

Charismatic leadership theory underpins trait theory and is based on the hereditary traits of the individual. The term „charismatic" was introduced in 1920 by Max Weber, the Greek kharisma translating as grace, native given (Duțu 2008, 14). For a competent and effective leader, charisma is not enough, but it is necessary, that is why programs are organized to develop the charisma of the military leader that involves self-criticism or engagement in the process of mentors trained in this regard.

Trait theory. Personality traits are factors that influence leadership success. These are the following: physical and constitutional factors (external appearance, age, height, weight), psychological (intelligence, communication, knowledge, character, self-esteem and self-control, perseverance, initiative), psychosocial (diplomacy, sociability, cooperation, popularity) and sociological (socio-economic status).

Oppenheimer, despite his introverted, reflective and often reserved style, manages to inspire and motivate his team, even with a tendency to be critical and self-critical alike. His intelligence and skills were essential in the development of nuclear weapons, both in physics and mathematics.

https://doi.org/10.53477/2284-9378-23-24

b) Behaviourist theories, in the late 1960s, include the two-dimensional behavioural theory and the behavioural continuum theory.
The two-dimensional behavioural theory – one as an expression of the type of leadership that oscillates between a permissive approach and excessive control, both of which have negative effects, and the second as an expression of the modern type of participative, consultative leadership, with emphasis on both the particular goals of the individual and those of the collective.

Behavioural continuum theories start from the autocratic style and descend to Oppenheimer's characteristic democratic style in which the leader encourages member involvement in decision-making.
Several aspects of Oppenheimer's leadership style and behavior can be linked to behaviorist principles. Behaviourist theories in management focus on behaviour and influence on organisational performance. These are found in Oppenheimer's charismatic communication style, his interpersonal relationships with his other team members of engineers and researchers, and his ability to inspire and motivate them to achieve the ambitious goals of the Manhattan Project.
With an adaptive intelligence, in an accessible and engaging manner, he was able to explain complex concepts to them and was appreciated by his colleagues for his modesty and sophistication.

c) Contingency theories include the theory of the favourability of the leadership situation, the theory of the maturity of subordinates (until the early 1980s);
Fred Fiedler's *contingency theory* – the association between leader orientation and group effectiveness is dependent (contingent) on the extent to which the situation is conducive to influence. Contingency approaches focus on the conditions for leadership success in different situations (Merce and Halmaghi 2003, 1). From this theory derives the observation that leaders are formed, not innate, each manager can achieve success if he builds through his own leadership style.

Although there appears to be no direct link between Oppenheimer and contingency theory, his leadership of the Manhattan Project took into account contingent factors such as available resources, and political and technical situations given by the involvement of various science and engineering specialists. His approach as a leader involved issues of adaptability and management of contingent factors in the context of nuclear weapons development.

d) The theories of new leadership are as follows: cognitive theories (normative decision-making theory, path-path theory, attribution theory) and social interaction theories (dyadic-temporal link theory, transactional leadership theory). These are valued by Oppenheimer in his relationship with his team members, a relationship in which he has cultivated collaborative cohesion, open communication and active involvement.

e) Situational theories include Robert House's route-to-goal theory and Hersey-Blanchard theory.
In the context of situational theories of leadership, Oppenheimer's model of work deployment and role in the Manhattan Program can be interpreted concerning the needs of team members and the adaptive style of the leader. The effectiveness of the leadership style depends on the maturity of the subjects, the pressures exerted, the level of security, the willingness to make an effort, and even the degree of confidentiality assumed.

Robert House's route-to-goal theory (Merce and Halmaghi 2003, 6) from 1977 – addresses situations in which the maximum effectiveness of various leader behaviours is achieved, combining the leader's traits with situational elements (crisis situations, uncertainties). The important activities of leaders are related to clarifying the routes to various goals such as promotions, personal achievements, pleasant working climate, all of which are of interest to subordinates. Achievement of these goals generates knock-on effects: *Job satisfaction à Acceptance lideruluià Willingness to work.*

Once this readiness has been achieved, the leader has a duty to keep the interest of subordinates alive, to stimulate them through rewards, and to guide and train them continuously. This can range from a guiding (directive), supportive (sensitivity to employees' needs), participatory (consulting subordinates' opinions) or achievement-oriented behaviour, where the leader emphasises encouragement, confidence and motivation.)
Hersey-Blanchard Theory of Situational Leadership or *Leadership Life Cycle Theory* – refers to the interdependence created between leadership styles and different situational contexts to ensure effective leadership.
To these are added *the theories of innovation* and *emotional awareness.*

3.3. Robert Oppenheimer and the power of leadership
Although late in the Second World War, the Americans managed to discover fission in the laboratory, bring it to the battlefield and temporarily hold a monopoly. In 1947, the Soviets succeeded in isotope separation of uranium by centrifuge, and on 10 June 1948, the first plutonium production reactor came into operation (Villain 2014, 36).

A physicist of genius and a man of integrity, J. Robert Oppenheimer was also a polyglot interested in philosophy, the interests of a precocious child continuing and developing into adult life. From his grounding in philosophy, with a well-defined awareness of a leader guided by ethics and responsibility, came the famous remark "Now I become Death, the destroyer of worlds", uttered during the first nuclear test, known as the Trinity Test, which took place on July 16, 1945, as part of the Manhattan Project. The phrase is a quote from a passage in the Bhagavad-Gita, an ancient Indian epic relevant to Oppenheimer at the time. A part of the epic Mahabharata contains

a dialogue between Prince Arjuna and the supreme Hindu god Krishna, describing Krishna's divine nature and warning that he will become, through war, the destroyer of worlds. Witnessing the explosion, the destructive power of the Trinity Nuclear Test impressed him and reminded him of the passage in the Bhagavad-Gita, hence his deep reflection on the ethical implications of developing nuclear weapons and his awareness of their devastating impact. He understands the intrinsic similarity to the destroyer god, assuming himself the role of an agent of destruction.
An undisputed visionary from his era, Oppenheimer had a well-defined strategy for the use of nuclear energy, understood the general implications, and promoted nuclear safety and the use of nuclear energy for peaceful purposes.

Based on the *Theory of Multiple Intelligences*, he stands out for his verbal-linguistic intelligence, his social and interpersonal intelligence, his abilities being put to good use in his actions by which he maintains group synergy, manages to persuade and motivate, understands emotions, mediates conflicts, demonstrating visible leadership qualities. He has a gift for oratory and is attentive to the meaning of the words chosen, the symbols and the intensity of the messages conveyed.

In his extensive recruitment drive, he has travelled all over the country to find and persuade the most talented scientists, mechanics, technicians and engineers to join the project. He used all his leadership skills, emotional and social intelligence, and stressed the urgency of the task. It was no easy task to persuade the best people to work at a remote military post in the middle of the New Mexico desert and live there with their families for the duration of the war.

Leadership qualities such as assertiveness, kindness and empathy were found in Oppenheimer as he supported his team through tough times when morale suffered from the stringent security requirements, fatigue from long hours in gruelling conditions, stress, and tension. Thus, together with other responsible coordinators in various departments, he has been concerned with organising recreational activities, increasing food facilities and ensuring good living conditions.

At first, recruits from the Universities of Princeton, Minnesota, Chicago or Wisconsin California arrived at Los Alamos in March 1943 with equipment essential to the process: two particle accelerators from Wisconsin, another from Illinois and a cyclotron from Harvard - a particle accelerator invented in 1934 by Ernest Lawrence, for which he was also awarded the Nobel Prize in 1939.

On April 1, 1943, Los Alamos was officially declared a military facility and Robert Oppenheimer was the scientific director, with recognized authority and administrative responsibilities. From his position of civilian authority, Oppenheimer established cooperative, not controlling, relationships with military personnel, an example being his close partnership with Colonel John M. Harman, the military chief who had responsibility for overseeing Los Alamos (Jones 1985, 86). The two

project leaders wanted to introduce various attractive work and living conditions, while General Groves wanted as much control over the scientists as possible. Groves even proposed appointing key civilian leaders as army officers, which aroused discontent and rumbling among the other scientists.

Choosing Oppenheimer as head of the Los Alamos lab was not easy, given that the other three heads of the other Manhattan labs – Ernest Lawrence, Arthur Compton and Urey - were all Nobel Prize winners. As an unproclaimed Nobel genius, although he applied three times for the famous scientific distinction – between 1945-1951 and in 1967 (Marcovici 2018, 42), he always managed to give more than he received, proving once again his unquestionable qualities as an absolute leader.

Nicknamed the *American Prometheus* (Bird and Sherwin 2006), Robert Oppenheimer is like the figure from Greek mythology, a titan who stole "*fire*" from the gods and gave it to mankind, at the cost of his peace. Just two months after Hiroshima and Nagasaki, shaken by the effects of the atomic bomb, he resigns from Los Alamos. He quickly realised the devastating effects of the atomic bomb used for political and military purposes, and that these actions were no match for his set of human principles and values. Oppenheimer is the epitome of the ultimate sacrifice, the man who experienced ecstasy and agony, all for the purpose of science.

Oppenheimer's work includes significant scientific contributions in the field of quantum physics, deep knowledge in nuclear weapons design and development, massive efforts focused on the Manhattan Project, which he led as technical director, and coordination of the team of engineers and scientists. His outstanding leadership and management skills inspired others to integrate the project as a shared mission with challenges and responsibilities.

Conclusions

Over the past century, scientific research in nuclear energy has evolved gradually from the founders of modern physics to the present day. Pierre and Marie Curie, daughter Irène, son-in-law Frédéric Joliot-Curie, and Henri Becquerel, the father of radioactivity, all Nobel Prize winners for their groundbreaking work, have laid the cornerstone for their discoveries in nuclear research. In that pioneering era, the harmful effects of reactivity were unknown; today, the pros and cons of atomic physics are being debated, with implications for the intentionality and orientations centred on military, economic and social interests, which could recalibrate the balance of power in the world.

ALSOS, part of the *Manhattan Atomic Project*, was under the civilian leadership of Professor Robert Oppenheimer and the military leadership of General Leslie Groves. To respond to the challenges thrown up along the way and to meet the feverish

debates, Oppenheimer's leadership is an art that aims to take account of moral values, individual and collective, to unite people in close cooperative relationships. It is an art when it is seen as the set of methods and procedures by which an individual motivates, persuades and leads other people to follow him even enthusiastically in the pursuit of a clear and well-defined goal. However, it is also science when methods and techniques are used as a result of research into the conduct of military action. Although a civilian, but also a man of atypical genius without a PhD, Oppenheimer had to think, behave and act like a military man, which is why we can extrapolate from civilian genius to military genius, especially given the importance of the military mission he was leading.

The leader encourages teamwork, the creation of a group identity, emotional intelligence being important in the processes of awareness, accessing and generating emotions. This virtuosity of intellect and feeling of the Oppenheimer leader also refers to the *military genius* proposed by Clausewitz in his *On War*. Military genius refers precisely to this "*harmonious union of forces*" (Clausewitz, 26) readily associated with all the qualities of the military leader. Of these, being visionary, generous, disciplined and a good communicator are the basic pillars of a solid leadership construct.

References

Atomic Heritage Foundation. 2014. "Alsos Mission." *National Museum of Nuclear Science & History.* https://ahf.nuclearmuseum.org/ahf/history/alsos-mission/.

Bird, Kai, and Martin J. Sherwin. 2006. *American Prometheus: The Triumph and Tragedy of J. Robert Oppenheimer.* Vintage Books.

Chrétien, Fleur. 2020. "Définition de leadership et différence avec le management." *CADREMPLOI.* https://www.cadremploi.fr/editorial/conseils/conseils-carriere/quest-ce-que-le-leadership-.

Clausewitz, Carl von. n.d. *On War.* Antet XX Press.

Duțu, Petre. 2008. *Leadership and Management in the Army.* Bucharest: "Carol I" National Defence University Publishing House.

Gosling, F. G. 2010. *The Manhattan Project. Making the Atomic Bomb.*

Iosif, A. 2009. "The atom. Dalton's atomic model." *SCIENTIA*. https://www.scientia.ro/fizica/63-atomul/262-atomul-modelul-atomic-al-lui-john-dalton.html.

Jones, Vincent C. 1985. *Manhattan: The Army and the Atomic Bomb (United States Army in World War II).* Washington DC: Center of Military History United States Army.

Marcovici, Ozias. 2018. *The atom between science and politics or from Los Alamos to Hiroshima.* Iași: Danaster Publishing House.

Marshall, Gordon, and John Scott. 2014. *Dictionary of sociology.* Bucharest: ALL Publising House.

Merce, Eugen, and Elisabeta-Emilia Halmaghi. 2003. "Contingency approaches to leadership." *Army Academy "Nicolae Balcescu" from Sibiu.* https://www.armyacademy.ro/biblioteca/anuare/2003/ABORDARI1.pdf.

Smith, Todd. 2020. "The Strategic Intelligence Triad: The differences between CI, BI, and KM." *Cipher.* https://cipher-sys.com/blog/the-strategic-intelligence-triad-the-difference-between-ci-bi-and-km?hs_amp=true.

Villain, Jacques. 2014. *Le livre noir du nucléaire militaire.* Librairie Arthème Fayard.

No.2/2023, APRIL-JUNE
https://doi.org/10.53477/2284-9378-23-25

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

The resilience of the military leader – defining traits and its ability to influence the operational environment

Lt. col. Marius-Iulian BADIU, Ph.D.*
Lt. Laura-Alexandra ȚICĂ**

*"Mihai Viteazul" 30th Guards Brigade, Bucharest, Romania
e-mail: badiumarius80@yahoo.com

**"Mihai Viteazul" 30th Guards Brigade, Bucharest, Romania
e-mail: laura.alex24@yahoo.com

Abstract

The military environment, by its very nature, is recognized as a source of occupational stress. The military's approach to measuring stressors, analyzing and comparing them with the capacity to cope, gives rise to both distress and eustress. Challenges arise when the effects of stress surpass an individual's ability to adapt, hindering their response to new demands. Military organizations highly value resilience as the key to effectiveness and success. In the military context, resilience can be viewed as a process, skill, or outcome, wherein military leaders exhibit the ability to confront fear, navigate outside their comfort zone, and overcome challenging moments in pursuit of a greater purpose.

Keywords:
operational environment; resilience; military leader; challenge; occupational stress; capacity.

Current military operations often take place in volatile, uncertain, complex, and ambiguous (VUCA) environments, along with cognitive overload, caloric deprivation, physical effort, and sleep restriction. Characterized by rapid and continuous change, military operations require military leaders' resilience and availability to maintain both physical and cognitive performance in stressful environments. Resilience has emerged as a critical skill in the military environment throughout history. In fact, the military were among the first to use this term to describe how people overcome the psychological trauma of war, dating back to World War I. Since then, the concept of resilience has evolved and developed into a multidimensional skill involving both psychological and social capacities. In the military environment, resilience has become a critical skill for survival, success, and protection against the trauma and stress of the operational environment. Military resilience is an important topic in both peacetime and wartime. During training and preparation, soldiers learn how to develop their skills and strengthen their ability to deal with difficult situations and manage stress (Cacioppo, et al. 2015, 93).

Acquiring resilience through psychological preparation and operational stress control

Psychological training and operational stress control are based on the realization and implementation of programs that include measures to identify, prevent and manage the reactions instigated by operational stress and building the resilience of the military. These effects are the result of both psychological training activities that focus on the development of individual effectiveness and activities that emphasize the control of stressors (Marineanu 2015, 12).

The psychological training of the military includes three stages: the mission preparation stage, the mission deployment stage, and the post-mission stage.

In the first stage, the training takes place by creating a motivating framework where group cohesion prevails and the soldiers are trained in relation to the negative effects they will face during the mission: exposure to very high temperatures, sleep deprivation, tiredness, and stress, but also other risks and situations they will face.

In the second stage, the emphasis is on analyzing the verbal and non-verbal behavior of the military which is correlated with deviant behaviors that were not observed in the first stage, traumatic events, emotional stress, mild craniocerebral trauma, where the psychologist has the role of taking all necessary measures to help the military successfully carry out their missions.

The third stage focuses on the reintegration of the military into the initial environment and the monitoring of the mental state to identify disorders arising from exposure to traumatic events and operational stress.

https://doi.org/10.53477/2284-9378-23-25

The reactions and effects on the military produced by operational stress are in fact, normal manifestations that occur at the body level following unexpected or unusual stimuli, their intensity being different. Depending on the intensities and the different ways in which they can exert influence, these reactions and effects can be adaptive or maladaptive (Kennedy 2006, 45).

In conditions where trust-based, cohesive, camaraderie relationships prevail within a unit or structure and there is effective management, the effect triggered by risk factors can be constructive, adaptive, and advantageous by improving performance both at the individual level and at the collective level in several directions:

- The evolution of personal relationships based on loyalty, trust and cohesion between soldiers who belong to the same hierarchical level;
- The evolution of relations between the soldiers and their commanders, which are all based on loyalty, trust and cohesion;
- The spirit of the corps by identifying the military with the principles and history of the unit or structure of which they are a part;
- Cohesion through interpersonal trust and knowledge established by the military, successful completion of common tasks even if they involve risks, understanding of responsibilities;
- Show courage by saving lives or even sacrificing your own life for the successful completion of the mission.

Maladaptive reactions are usually manifested by mental disorders: extreme anxiety, violation of military regulations or panic. Reactions and effects produced by operational stress can be mild and temporary or severe and with a longer period of manifestation, and approaching them in an unconscious way and not treating them in time can lead to their permanence.

In the military environment that is characterized by complexity and continuous change, it is very important for the military to gain resilience, a fact that proves the inner strength and courage to face the multilateral character of actions and the fear that arises during the conduct of missions. Resilience is the military's ability to adapt emotionally, mentally, spiritually and behaviorally, in combination with mental, physical and social skills to perform favorably. Psychological preparation and control of operational stress are grounds for performance and stability at the collective level and strengthen the military's resilience to face mental and physical challenges (Horowitz and McIntosh 2018).

Introduction to the concept of resilience

Resilience is defined as "*a continuous and repetitive process, the purpose of which is to protect a given system and allow it to address the changes that have occurred. For this, resilience involves, firstly, combining the already existing features of the system*

(existing programming) with various risk management approaches and, secondly, capitalizing on a set of capacities to strengthen resilience itself (adaptation, absorption, transformation)" (Mitchell 2013, 4-5).

Boris Cyrulnik defines resilience as *"the human capacity to resist, recover and rebuild despite the occurrence of one or more traumas.*" (Cyrulnik 1999, 2). Resilience is also "*viewed, on the one hand, as a characteristic of the person who has experienced or is experiencing a traumatic event or chronic adversity and brings a good ability, and on the other hand, it is viewed as the result of an interactive process between the person, the family and the environment"* (Ionescu and Blanchet 2006, 159).

Resilience can be analyzed as a process, skill or as result. Resilience as a process is perceived as returning to normal functioning with the help of protective factors after facing an internal stressor. Resilience as a skill defines a military person's ability to adapt appropriately to stressful events and changes. Resilience as a result brings to the fore the beneficial and positive effect that results from facing and going through stressful events. A resilient leader obviously possesses the following qualities: quick adaptation to new situations, flexibility, ability to keep calm and stay optimistic in critical situations; he is empathetic and trusts his own intuition, finding solutions to problems that arise, etc. (Arnold, et al. 2014, 6).

The role of resilience in current military operations

Military resilience can be defined as the ability to overcome the negative effects of setbacks and stress associated with combat effectiveness and military performance.
In the volatile, uncertain, complex and ambiguous (VUCA) operational environment, both current and future operations demand and place greater priority on improving and sustaining military readiness and resilience to succeed in the missions assigned. Resilience is a necessity for every person, but especially for those who work in fields with a high degree of risk and where they face effort and stress, one of these fields being the military field. The complex training specific to the military environment, the tactical applications and the exercises in which the soldiers take part are both physically and mentally demanding. International missions have a high degree of risk where psychological stress, emotional trauma and physical health hazards prevail that can affect participants due to the experiences they are subjected to; thus, developing resilience, strengthening inner strength and psychological preparation are paramount for today's military. To increase military resilience, emphasis must be placed on existing skills (the ability to survive in combat and mental and physical characteristics), managing the negative effects of stress, and the ability to face the fear of injury or loss of life (Fletcher and Sarkar 2013, 18).

Resilience is a key skill for the military as they must be prepared to face the challenges and uncertainties that characterize the operational environment. Soldiers

https://doi.org/10.53477/2284-9378-23-25

have to face stressful factors and maintain their ability to act in critical situations. Resilience is the indispensable ability for military personnel to overcome their limits and recover from negative or stressful events, maintain their balance, and continue their mission despite difficulties.

For the military, resilience can mean the difference between life and death, between success and failure in a mission. In the military environment, situations can be extremely stressful and dangerous, with critical decisions that must be made in a limited period of time. The military is constantly exposed to uncertainty, risks and threats, but must find ways to act and deal with them. By developing resilience, soldiers are given skills to better face challenges and maintain high-performance levels. A resilient military leader can make informed decisions, think strategically, and successfully manage the team in unpredictable or difficult situations. He will be able to stay calm and maintain his focus in critical moments, find the necessary resources to overcome difficulties and be able to communicate effectively with team members (Simmons and Yoder 2013).

Resilience in the operational environment refers to the military's ability to adapt quickly and effectively to changes in the operational environment and to recover quickly from unexpected events or crisis situations. In an operational environment, military personnel face numerous challenges and uncertainties, including risks to their safety, environmental hazards, and operational constraints. Resilience is important to the military because it allows them to maintain their effectiveness and mental and physical health in the harsh conditions of the operational environment. The ability to quickly adapt to the new situation and quickly develop new skills and strategies is crucial to success during a mission.

Resilience focuses on the behavioral, emotional, spiritual and mental adaptability of soldiers and is a necessary trait to cope with difficult times characterized by stress. Resilience also refers to the power to accept failure and learn from mistakes, to accept the positive or less positive consequences of actions committed, and the manner in which a soldier is able to face challenges outside the area of comfort and face their fear to act in difficult moments and control their full energy and capacity are real challenges.

Decisional resilience of the military leader

The decision-making resilience of the military leader can be defined as his ability to deal with tense situations and stresses in the military environment, to make quick and well-founded decisions in critical situations, as well as to maintain his concentration during the decision-making process.
Decisional resilience is a key skill for military leaders, who must be able to quickly evaluate their options and make well-informed decisions under pressure. Such

leaders have the ability to remain calm and centered during difficult situations and to find practical and effective solutions to the problems encountered (Allison 2011). Likewise, a military leader with well-developed decision-making resilience can motivate his team and communicate effectively with its members in situations under pressure. These leaders can also take responsibility for the decisions made and manage the risks involved well. This skill also involves the ability to adapt to unexpected changes in the operational environment, evaluate information and take risks, but also learn from failures and continuously improve his leadership qualities.

The military leader's decision-making resilience can be developed through adequate training, crisis simulation, and the cultivation of skills such as taking responsibility, delegating tasks, effective communication, and strategic thinking. A military leader's ability to be resilient under pressure can be crucial in efforts to protect the lives of subordinates and successfully complete assigned missions.

To develop and maintain strong decision-making resilience in the operational environment, the military leader must meet certain requirements and develop key skills such as:

1. Situational awareness – The military leader must be able to quickly assess the situation and gather relevant information to ensure that his decisions are appropriate and well-founded;

2. Goal orientation – The ability to set clear goals and focus one's efforts on them is important to avoid wasting time and energy;

3. Critical thinking – Critical thinking and the ability to examine arguments and opinions objectively contributes to making more sensible decisions based on logical reasoning;

4. Flexibility – Flexibility is vital in the operational environment. The military leader must be willing to adapt his plans and decisions as the situation evolves;

5. Confidence in oneself and subordinates – Confidence in oneself and one's subordinates is fundamental to decision-making resilience. The military leader must have confidence in his own decision-making abilities and ensure that his subordinates feel equally confident in them at all times;

6. Experience – experience in making decisions and completing previous missions can improve a military leader's ability to act quickly and effectively in critical situations;

7. Emotional intelligence – Military leaders must be able to understand their own emotions and those of others, manage their stress, and remain calm in tense situations.

By developing and maintaining these characteristics and skills, a military leader can successfully meet the challenges of the operational environment and make effective decisions that will help them accomplish their goals and achieve success in their missions.

Final considerations

Resilience is present at all levels of organizations and is a capacity that can be enhanced. However, its absence can be viewed as a vulnerability, both at the individual and organizational levels.

By default, the operational environment is characterized by threats and dangers, which often present dramatic obstacles for individuals, some of which directly endanger their lives. Therefore, increasing the resilience of military personnel should be a priority for all members of the military, irrespective of their hierarchical level. Modern armies have begun to implement programs to develop military resilience, starting with the military in training courses (MRT- Master Resiliency Training in the United States of America or Battle Smart in Australia), up to the military at the highest hierarchical levels. Practicing techniques and ways to increase resilience enables all military personnel to face difficult and critical situations in their pursuit of successful mission completion.

In other words, resilience is a fundamental skill in the military environment and plays a critical role in military survival and success in challenging conditions. This includes training, developing, and continuously improving psychological and social skills needed to effectively and efficiently deal with crisis situations and the inherent stress of the military environment.

References

Allison, Elle. 2011. "The Resilient Leader." *The Resourceful School* 69 (4): 79-82. https://www.ascd.org/el/articles/the-resilient-leader.

Arnold, Margaret, Robin Mearns, Kaori Oshima, and Vivek Prasad. 2014. *Climate and Disaster Resilience: The Role for Community-Driven Development.* Washington DC: Social Development Department. World Bank.

Cacioppo, John T., Amy B. Adler, Paul B. Lester, Dennis McGurk, Jeffrey L. Thomas, Hsi-Yuan Chen, and Stephanie Cacioppo. 2015. "Building social resilience in soldiers: A double dissociative randomized controlled study." *Journal of Personality and Social Psychology* 109 (1): 90-105. doi:https://doi.org/10.1037/pspi0000022.

Cyrulnik, Boris. 1999. *Un merveilleux Malheur.* Paris: Odile Jacob.

Fletcher, David, and Mustafa Sarkar. 2013. "Psychological resilience: A review and critique of definitions, concepts, and theory." *European Psychologist* 18 (1): 12-23. doi:https://doi.org/10.1027/1016-9040/a000124.

Horowitz, Jonathan, and Diane McIntosh. 2018. *Stress: The Psychology of Managing Pressure.* London: Dorling Kindersley Limited.

Ionescu, Șerban, and Alain Blanchet. 2006. *Tratat de psihologie clinică și psihopatologie.* București: Editura Trei.

Kennedy, Carrie. 2006. *Military psychology – Clinical and Operational Applications (First Edition)* . New York: Guilford Press.

Marineanu, Vasile. 2015. *Manual pentru pregătirea psihologică și controlul stresului operațional.* București: Editura Centrului Tehnic-Editorial al Armatei.

Mitchell, Andrew. 2013. "Risk and resilience: from good idea to good practice." *OECD Development Co-operation Working Papers,* No. 13. https://www.oecd-ilibrary.org/docserver/5k3ttg4cxcbp-en.pdf?expires=1684750190&id=id&accname=guest&checksum=86E3226073DFDBB4476AB6EAD396B168.

Simmons, Angela, and Linda Yoder. 2013. "Military Resilience: A Concept Analysis." *Nursing Forum* 48 (1): 17-25. doi:https://doi.org/10.1111/nuf.12007.

No.2/2023, APRIL-JUNE
https://doi.org/10.53477/2284-9378-23-26

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Intelligence support for the operational level counter-deception

Maj. George-Ion TOROI, Ph.D. Candidate*
Col. Cristian-Octavian STANCIU, Ph.D.**

*"Carol I" National Defence University, Bucharest, Romania
e-mail: george_toroi@yahoo.com
**"Carol I" National Defence University, Bucharest, Romania
e-mail: cristianstanciu73@yahoo.com

Abstract

Given modern warfare's complex and dynamic nature, military deception has become a vital tool in the contemporary operating environment for gaining strategic advantage and achieving operational success. For this reason, countering enemy deception operations has become an operational requirement to support mission accomplishment. Furthermore, with the increased use of modern technologies and information warfare tactics by adversaries, intelligence has become a critical asset in countering enemy deception operations and protecting the safety and security of military personnel and operations. The Russian-Ukrainian ongoing war has proven once again that deception remains a viable tool in the contemporary operating environment and can still have a huge impact on the battlefield. Considering its value, this article explores approaches to diminish and counter the impact of deception at the operational level of war. Moreover, our research explores how the joint function of intelligence can support the efforts of counter-deception throughout its entire process.

Keywords:

deception; counter-deception; information; detect; Russia; war.

Introduction

„*All warfare is based on deception*" is one of the oldest and well-known aphorisms in the military domain. History has proven countless times that, indeed, deception has been a critical aspect of warfare regardless of the period. By creating confusion and uncertainty in the enemy's mind, protecting friendly forces and assets, exploiting the enemy's vulnerabilities and weaknesses, and reducing friendly casualties, deceit has played a crucial role in ensuring operations success.

It has been proven by centuries of historical examples that military deception can provide numerous benefits to armed forces, including achieving surprise, disrupting the adversary's decision-making process, protecting critical information, enhancing operational security, and improving the effectiveness of military operations. For this reason, nowadays, regardless of the technological development of intelligence sensors, deception remains a powerful weapon in order to gain operational advantages on the battlefield. Nowadays, the majority of the western military doctrines still recognize its relevance: „*No major operations should be undertaken without planning and executing appropriate deceptive measures*". (AFM 2018, 3A-1)

The impression that possessing evolved collection assets can bring about full clarity on the operational situation is a false one. Not only is it erroneous, but it furthers amplifies the possibility for successful enemy deception by creating preconceived ideas, thus vulnerabilities for the enemy deceit to exploit.

The main reason why deception remains effective regardless of the sensors' evolution is simple: capitalizing on the vulnerable aspects of the psychological dimension of human nature is the main characteristic of misleading actions. Therefore, the enemy's mind is the target of these operations, and as long as the human brain is susceptible to error, the chances of a successful deception remain constant.

NATO recognizes deception as one of the military drivers in today's operating environment. „*Our adversaries will seek to present the Alliance with multiple dilemmas through deception and by sowing confusion across the continuum of competition*" (AJP-01 2022, 37). Furthermore, NATO members are extremely aware of their adversary's experience with respect to employing deception: „*Russia views deception (Maskirovka) to be a vital precursor to success*" (AFM 2018, 3A-4). However, in our humble opinion, NATO doctrine does not adequately address the subject in accordance with its importance. There is no dedicated NATO document to explore the counter-deception process, regardless of the level of war. Moreover, Allied Joint Doctrine for Operations Security and Deception, although relatively recently approved, in March 2020, dedicates only half of page to counter-deception. This being said, there is much room for improvement in the Alliance when it comes to addressing such a sensitive and important aspect of any military operation. This represents a crucial aspect at any

level of war, but more importantly at the operational level, where Joint HQs need to integrate effects and counter enemy actions in multiple operational domains.

Furthermore, although one of the functions of intelligence is to counter enemy deception operations and surprise (AJP-2 2020, 1-3), none of the NATO intelligence functional doctrine addresses this issue separately. There are indeed sporadic references to this in the NATO "Information" documents, but no coherent and logical approach to countering adversary deception can be found in any of these works.

In light of this, our research's primary question is the following:
- *How can intelligence joint function support the counter-deception process?*
For this reason, our article explores how intelligence can better support the counter-deception process and tries to raise awareness amongst NATO commanders and intelligence specialists with respect to the lack of doctrinal foundation on this subject. In addition, the present paper also offers a procedural framework as a solution to the identified problem, which should constitute the subject of future quantitative research to validate and develop it in order to apply it at the operational level of armed conflicts.

Based on the primary question stated before we developed several subsequent questions to help us solve the problem identified:
- *Is counter-deception a critical operational requirement considering the features of the contemporary operating environment?*
- *How should counter-deception work? What is the process of countering deception?*
- *What is the intelligence role in this process? How can intelligence joint function support the counter-deception process?*
In this respect, we divided the topic into several logical steps that should provide answers to the research questions.

First, we analyzed whether deception is still a valid operational concept in today's conflicts in order to see if efforts to develop a counter-deception doctrine are required. Furthermore, using a multidisciplinary analysis we provided some essential benefits of countering deception in support of military operations. Next, using the qualitative research methods of content and comparative analysis we performed a thorough introspection within NATO and some other Western nations' doctrines to see how counter-deception is addressed. Moreover, we made an analysis of their respective deception doctrine in order to develop countering methods to the essential deception concepts identified. Using an inductive method, we then reconstructed the conclusions obtained from the deception analysis into a counter-deception process.
In the end, based on the already recognized intelligence functions, using deduction, we depicted those specific intelligence-related activities that need to be performed within every phase of the counter-deception process.

1. Counter-deception – an essential operational requirement

The well-known aphorism presented at the opening of the introduction, „*all warfare is based on deception*", is attributed to Sun Tzu as part of his work, The Art of War. It represents a saying more than two millennia old and serves as a constant reminder that deception is a key component of war. By remaining unpredictable, it is often possible for one side to outsmart their opponents, even when chances are not favorable.

In order to gain an advantage over the enemy, military commanders have employed various forms of deception throughout history, such as misdirection, feints, or false information. As such, deception has been a part of warfare since ancient times and continues to play a significant role in modern conflicts. The multitude of successful examples is the main reason why Sun Tzu's aphorism has remained operationally viable for so long. Considering all of this, deception should be recognized as an integral part of the nature of war, and those engaged in military planning must be aware of its potential within the overall concept of operations.
Furthermore, nowadays, the operating environment, characterized by an abundance of information, rapid communication, global reach, technology dependency, or hybrid tactics, presents significant opportunities for deception operations to be carried out effectively.

At the same time, based on the technological development of intelligence sensors, as part of the contemporary environment, one might conclude that deceiving has become almost impossible. While, indeed, recent technological advancements in Intelligence, Surveillance, and Reconnaissance (ISR) capabilities have greatly enhanced military intelligence-gathering capabilities, it would be a mistake to assume that deception is no longer viable in modern warfare. Deception remains an effective tactic in military operations, especially when it is executed creatively and adaptively to exploit the cognitive weaknesses of the enemy.

In addition, it is important to underline that, while technological advancements have enabled military forces to collect and process vast amounts of data, this data is not always complete, accurate, or timely. Consequently, the resulting level of situational understanding is often truncated, which provides opportunities to mislead the opponent. Moreover, the increasing complexity of modern conflicts and the rapid pace of technological change mean that there will always be opportunities for deception to be used effectively.

Therefore, it is important for military commanders and intelligence analysts to recognize the ongoing threat posed by deception and to develop and implement effective counter-deception strategies. This requires a multi-disciplinary approach that integrates technological solutions, analytical expertise, and operational experience. Ultimately, by maintaining a clear-eyed understanding of the continuing

threat posed by deception, military forces can better prepare themselves to defend against and counter enemy deception operations.

Furthermore, the ongoing conflict between Russia and Ukraine has proven deception to be a key enabler for success on either side. At the operational level, the most conspicuous example might be considered the Kherson ruse employed by the Ukrainians in September 2022, as part of their counteroffensive. The rapid advancement and the vast territorial gains of the Ukrainians have proven deception to be a very effective shaping operation, regardless of the Russian ISR technological development.

Moreover, deception viability in the contemporary operating environment is demonstrated by the interest of Western actors in deception operations. Many of the important allies and NATO itself have recently developed doctrines that address this key enabler of modern operations. The table below highlights some of the doctrines and their release year in order to support our previous statement.

TABLE no. 1 Deception doctrines

Actor	Releasing year	Document
NATO	**2020**	***, AJP 3.10.2, *Allied Joint Doctrine for operations security and deception*, edition A, version 2, NATO Standardization Office
US	**2017**	***, JP 3-13.4, Military deception, US Joint Chiefs of Staff
US	**2019**	***, FM 3-13.4, *Army Support to Military Deception*, US Department of the Army
UK	**2018**	***, Army Field Manual - Warfighting Tactics Part 1: The Fundamentals, UK Ministry of Defence - *Annex A addresses the subject of deception*
ROU	**2021**	***, S.M.Ap. – 55, *Romanian deception doctrine*, Defense Staff, Bucharest

Additionally, deception represents a successful method that can bring a lot of benefits for the deceiver. It is a valuable tool for any military operation as it can create confusion, disrupt enemy plans, conceal intentions and capabilities, and ultimately increase the probability of success in achieving operational objectives.

Deception can be used to surprise the enemy by concealing intentions and operations, allowing military forces to gain the upper hand on the battlefield before the enemy can respond. It can also enhance security by misleading the enemy about the location and strength of military forces, protecting them from attack and preserving their combat power. Furthermore, deception can support creating opportunities for military forces to maneuver and operate freely in some operational areas by distracting the enemy's attention and effort. In addition, deceit might also be employed to conserve resources and minimize risk by fooling the enemy about the size and scope of military operations, allowing forces to achieve objectives with fewer resources and reducing the likelihood of casualties. All of these make deception a very valuable and sometimes cheaper tool for operational planners.

Furthermore, Russia, NATO's most significant threat, sees deception as a huge enabler of its operations. „The Russian Federation is the most significant and direct threat to Allies' security and to peace and stability in the Euro-Atlantic area" (NATO 2022, 4; JP3-13.4 2017). Russia is well-known for employing maskirovka within its military operations

Maskirovka is a Russian military doctrine that involves the use of deceit, camouflage, and concealment to support military objectives. It has been a central component of Russian military operations for many years and it is often used to confuse and mislead the enemy, protect Russian forces, and achieve operational objectives. Maskirovka can involve a range of tactics and techniques, including the use of decoys, false targets, disinformation, and psychological operations, among others. The goal of Maskirovka is to create uncertainty and confusion among the enemy, allowing Russian forces to gain the advantage and attain their objectives with minimal risk and cost.

Consequently, taking into account the above arguments, it becomes mandatory for all military forces to develop effective procedures to counter the deceptive actions carried out by their adversaries, so that the achievement of their own mission is not jeopardized. Furthermore, counter-deception can provide several benefits to military organizations:

- Maintaining operational security: Military counter-deception can maintain operational security (OPSEC) by detecting and neutralizing adversary deception operations. By identifying and countering adversary deceit, military organizations can prevent the adversary from exploiting vulnerabilities within its own concept of operations and protect the safety and security of military personnel and assets.
- Enhancing situational awareness: By identifying and exploiting the adversary deception, military organizations can gain insight into adversary capabilities, intentions, and activities, which can inform decision-making and enable operational advantages.
- Improving decision-making: Military counter-deception can improve decision-making by providing accurate and timely information about adversary capabilities, intentions, and activities. Based on the information obtained as a consequence of countering enemy deception, military organizations can reduce uncertainty and make informed decisions based on reliable information.
- Enhancing operational effectiveness: Military counter-deception can enhance operational effectiveness by neutralizing adversary deception operations and enabling military organizations to accomplish their mission with greater efficiency and effectiveness. It ensures maintaining the initiative and gaining the ability to dictate the course of events in accordance with its own concept of operations. Moreover, efficient counter-deception can create operational opportunities to double-cross the enemy, thus providing a more viable approach to solving the problem and fulfilling the mission.

It is obvious that military counter-deception can provide many benefits to the operational commander. Recognizing this, military organizations can enhance their ability to achieve operational success and protect the safety and security of military personnel and resources.

Considering the arguments provided in this section, it becomes evident that military counter-deception should be considered an essential operational requirement, as the use of deception by adversaries can pose significant threats to military operations and mission success. Effective counter-deception measures are necessary to detect, disrupt, and neutralize enemy deception efforts, thereby enabling military forces to maintain situational awareness, protect critical assets, and accomplish their objectives with greater efficiency and effectiveness. In this respect, developing a proper counter-deception framework becomes an operational necessity for any force.

2. Counter-deception process

As demonstrated before, counter-deception is a critical operational requirement in modern conflicts, given the significant role that deception plays in an operating environment characterized by features such as instant communication, information overload, and technology dependency. Effective counter-deception requires a multi-disciplinary approach, incorporating intelligence gathering, analysis, and dissemination, as well as specialized operations personnel and skills to exploit the opportunities that might arise from detecting the enemy's deceptive intentions. By developing and implementing a robust counter-deception process, military forces can better protect themselves against the negative impacts of enemy deception, and gain an operational advantage over the enemy.

First of all, in order to substantiate such a process, we consider it mandatory to understand the definition of counteracting the misleading actions of the adversary. To this end, „*counter-deception is an effort to detect, confirm, and subsequently negate, neutralize, or diminish the effects of, or gain advantage from, a foreign deception operation*" (JP3-13.4 2017, VII-1).

We would also like to point out that our analysis of this concept's definition has brought to light the conclusion that there is a great deal of synchronization in the Western way of thinking in relation to the definition of countering misrepresentation. Also, an in-depth examination of these approaches highlights the existence of three main phases of a potential counter-deception process: detection, confirmation, and exploitation, as outlined in the US military's deception doctrine (FM3-13.4 2019, A-1 – A-2). However, we consider it opportune, at this moment, to mention the fact that NATO does not address, in any of its doctrines, the process of countering deception, so the previously presented stages, specific to the American vision, are not implemented in the Alliance's documents.

Understanding the fundamentals of military deception is essential to developing effective countermeasures. It is impossible to neutralize the effects of any phenomenon if you do not develop a comprehensive understanding with respect to how it works. „*As the role of deception is expanding, the importance of implementing methods of countering deception is increasing. This requires a more thorough understanding of deception processes to implement counter-deception methods*" (Bennett and Waltz 2007, 2). Military deception is a complex and multifaceted concept that involves the use of a range of tactics and techniques to deceive the enemy. To effectively counter deception, military forces must first have a thorough understanding of the principles and fundamentals of deception, including the various types of deception, the methods, means and specific techniques. With this knowledge, military forces can develop effective counter-deception strategies that allow them to portray the benefits previously presented.

This was actually the procedure we used to develop our proposed process of counter-deception which enhances the one US uses and was previously presented. We do recognize the three phases the US process incorporates, but, in our opinion, to enhance the probability to counter enemy deception, military organizations should follow a five-phase process. We have added two more before the three US employs: counter-deception preparation and deception deterrence. The reason for including preparation is that it covers a set of activities that will enhance the probability of deception detection. Deterrence, on the other hand, helps forces to counter enemy deception by not portraying suitable conditions for them to make use of such methods. The process follows a logical flow, each phase playing a critical role in countering enemy deception.

The first phase, counter-deception preparation, involves developing and implementing measures to reduce the effectiveness of enemy deception. This phase includes an analysis of the enemy, the situation, and its own forces from the deception point of view. Identifying potential deception scenarios, the enemy's deceptive experience, but also its own vulnerabilities constitute some of the activities within this phase.

The second phase, deception deterrence, involves creating a credible deterrent to enemy deception. This phase includes planning special activities designed to make it difficult for the enemy to successfully execute their deception plans, thus determining them to give up own deceptive intentions. For example, NATO recognizes some suitable situations when there is a high probability to employ deception (AJP3.10.2 2020, 25). From a counter-deception perspective, not portraying to the enemy these operational situations on the battlefield can lead to the enemy not employing deception in their concept of operation, due to the increased risk it might imply.

The third phase, detection, involves identifying indicators that the enemy is attempting to deceive our friendly forces. This phase involves a substantial focus

on intelligence structures. In this sense, all subsequent processes of the information cycle contribute substantially to increasing the chances of identifying the adversary's deceptive actions. To this end, knowing one's own ISR capabilities, but also their limitations, as well as employing appropriate methods of analysis and processing of collected data is a "*sine qua non*" condition for the success of countering the adversary's deceptive actions at this stage of the process.

The fourth phase, deception confirmation, involves confirming all the details of the enemy's deception plan. Activities within this phase are of critical importance for exploiting the detection of enemy deceit. Without proper details regarding its plan, one cannot exploit the opportunity created by the detection phase.

The final phase, exploitation, involves using the information gathered during the previous phases to develop a double-cross plan. This phase includes exploiting the weaknesses in the enemy's deception plan and developing strategies to create operational battlefield advantages.

As a partial conclusion, we consider this counter-deception process an essential part of military operations. It provides a structured approach to countering enemy deception and ensuring the success of military missions. By following the five phases of the process, military organizations can effectively prepare, deter, detect, and exploit enemy deception to gain a decisive advantage on the battlefield. Further on, based on this process, we will identify how the joint intelligence function can support countering enemy deception operations.

3. A framework for intelligence support to counter-deception process

„*Deception is one of the biggest challenges in intelligence collection and processing. A well-organized attempt of deception by an adversary or any other actor may be difficult to reveal*" (AJP-2 2020, 2-13).

Therefore, deception poses significant challenges to the intelligence structures and processes. In intelligence operations, the collection of relevant data and its correct analysis and interpretation are essential in order to inform decision-makers and support the achievement of mission objectives. However, deceptive tactics employed by adversaries can undermine the accuracy and reliability of intelligence, making it difficult to distinguish between truth and falsehood. Deceptive practices can take many forms, including disinformation campaigns, false flag operations, and covert operations designed to mislead intelligence collectors. Such efforts can lead to the misinterpretation of data, false conclusions, and the allocation of resources based on incorrect assumptions. As such, intelligence professionals must remain vigilant to the potential for deception, and employ specialized tools and techniques to identify and neutralize deceptive tactics. This section represents general guidance

for intelligence structures in order to support each phase of the counter-deception process presented before to enhance the probability of its success.

3.1. Intelligence support to counter-deception preparation

As previously presented, preparation plays a huge role in the counter-deception process. The main role of the joint intelligence function in this phase is to provide updated information on the enemy and the situation in order to support the next steps of this process. The intelligence generated within this step is critical for the overall success of the counter-deception process. Much of this information should be obtained by the intelligence structure as part of the JIPOE (Joint Intelligence Preparation of the Operating Environment). The following are types of intelligence that should be generated within this phase:

- enemy mission, intent and distinct features of its operational art;
- enemy cultural and organizational factors;
- profiles of significant adversary decision-makers, including examinations of their professional backgrounds and experiences;
- enemy experience in deception operations;
- enemy doctrine and tactics specific for deception;
- limitations and capabilities with respect to deception;
- possible suitable situation for the enemy to employ deception;
- analyzing and identifying specific vulnerabilities with respect to our own information support process, including the elements specific to the preconceptions and prejudices of the personnel involved in this process and which can be exploited by the adversary.

3.2. Intelligence support for deception deterrence

Deterrence requires hiding elements essential for the enemy in order to develop successful deceptive plans. Establishing and implementing effective OPSEC measures are essential for the success of this phase. Although intelligence structures are not in the lead for this phase, they play an important part as they should provide information on the enemy's current knowledge of friendly disposition and intentions. Furthermore, during execution, the intelligence function should provide information on the operational situation and identify suitable situations in which the enemy may employ deception.

Moreover, intelligence support can be crucial in deterring deception, as it can provide early warning of potential deception attempts, enabling organizations to take proactive measures to deter or mitigate the effects of such efforts.

3.3. Intelligence support for deception detection

Deception detection requires, first of all, an understanding of the operational situation in order to separate true from false information out of the multitude of indicators that the enemy portrays on the battlefield. The level of understanding resulting from the collection and analysis of the information presented in the first stage of this process is a crucial factor in the effort to detect the deceptive actions of

the adversary. The motivation is extremely simple. The multitude of data collected during the operation is analyzed and interpreted in relation to the previous level of situational awareness. Cases that differ from the natural development of a regular adversary operational approach should constitute question marks for one's own intelligence structures regarding possible deceptive actions by the adversary. The identification of these incongruities is therefore the foundation by which the adversary's deceptive intent can be detected.

For these reasons, „*the detection of deception against friendly forces is a J2 responsibility*" (AJP3.10.2 2020, 5). Intelligence structures are the ones responsible for identifying specific indicators of enemy deception. An adequate intelligence cycle should be able to complete this task. However, there are several important recommendations that intelligence staff should apply:

- when it comes to identifying deceit, collection is not enough. It is important to have sensors that provide data, but, without proper processing, it is almost impossible to detect sophisticated deception operations;
- all collection capabilities have limitations and vulnerabilities that can be exploited by the enemy. If time permits, cross-checking data provided by multiple intelligence collection capabilities should be performed. „*While the level of detail in a single-source report could sometimes be sufficient to meet more immediate and narrowly defined requirements, all-source reporting is essential to gain in-depth understanding and avoid deception and misinformation*" (AJP-2 2020, 2-11);
- source reliability should always be analyzed;
- applying suitable structured analytical techniques has proven to be very useful in sorting out whether or not the deception is occurring (Moore 2015, 6);
- intelligence staff should always adopt a skeptical approach to all the collected data. There should be no shortages when it comes to analyzing these data;
- intelligence staff should always be aware of some barriers, either technical or human, such as cognitive limitations or personal biases and preconceptions;
- a very important aspect of detection is that intelligence resulted from processing data should always be compared to the one developed during the preparation phase in order to identify incongruities, which constitute the basis of deception detection.

3.4. Intelligence support to deception confirmation

Confirmation of the enemy's entire deception plan is essential to developing strategies to counter it. However, in order to choose the optimal option to capitalize on the opportunity created by detecting the adversary's deceptive indicators, it is necessary to develop a thorough understanding of his entire plan. Data must be collected on the scenario employed, methods and techniques, but also the level of progression and effectiveness of his plan so far. Equally, it is necessary to carry out an analysis of the effects created by misleading the adversary so far on our forces, but also of the effects that, according to the plan, it expects to achieve further on.

In order to be able to turn the situation into a vulnerability for the adversary, it is necessary to encourage his beliefs that his plan is working within the anticipated limits, and therefore correct knowledge of his future actions is a must.

The intelligence function should provide the necessary level of understanding in this regard. Identifying and prioritizing information requirements is of great importance to obtain essential data about the enemy's deception plan. In addition, it is important that this entire information cycle be extremely discreet so as not to give clues to the enemy that his plan has been debunked.

3.5. Intelligence support to exploitation

„*The response to the detection of deception against friendly forces is a command-led J3/5 responsibility*" (AJP3.10.2 2020, 5). Based on the situational understanding provided by the information processed in the earlier stages of this process, a series of options can be developed that the staff must analyze in relation to the established mission objectives and propose to the commander. „*Based on risks, commanders can ignore, expose, exploit, or defeat enemy deception efforts*" (FM3-13.4 2019, A-2). Regardless of the decision, intelligence can support any of the approaches.

Perhaps the most challenging option for information structures is the exploitation of the opportunity created. This essentially involves playing a double-deception on the adversary by developing plans that encourage his false belief with regards to the effectiveness of his actions, plans that, at the appropriate time, support achieving the operational surprise.

We consider it appropriate to emphasize again that the present process works in a logical and cascading progression, in such a way that the information developed in the early stages is essential for the success of the later ones. Therefore, in the case of this last stage of the counter-deception process, all previous data, especially those identified in the first and fourth stages, are extremely important in developing viable options for capitalizing on the operational situation created.

Conclusions

As a conclusion, it goes without saying that intelligence support to operational level counter-deception is a critical component of military operations. By identifying and countering enemy deception efforts, intelligence analysts can help ensure that military operations are successful and that personnel are kept safe. To this end, applying a structured framework to prepare, deter, detect, confirm, and exploit enemy deceit is mandatory.

One of the most prominent experts in the field of military deceit, Barton Whaley, came to the following conclusion in one of his studies: „*Indeed, this is a general*

finding of my study–that is, the deceiver is almost always successful regardless of the sophistication of his victim in the same art" (Whaley 1969, 76). For this reason, the need to come up with an effective counter-deception process is paramount. Furthermore, the scientific literature dedicated to deception acknowledges that *„the operational level commander is vulnerable to adversary deception and should formalize an internal systemic deception recognition process*" (McPherson 2010, 1). In this respect, the intelligence framework that we provided represents an effective approach to countering enemy deception operations.

Moreover, considering the evidence related to the employment of deceit in contemporary operating environment, this article intended to raise awareness within NATO with respect to the enemy employment of deception operation and the need to develop proper strategies to defend against these types of operations. Only with appropriate tools can the operational advantage so needed in modern conflicts be obtained, and the proposed process can represent one of these tools in terms of effectively countering the misleading actions of the adversary.

References

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

AJP-01. 2022. *Allied Joint Doctrine, Edition F, Version 1.* NATO Standardization Office.

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

AJP3.10.2. 2020. *Allied Joint Doctrine for operations security and deception,ediția A, versiunea a 2-a.* NATO Standardization Office.

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

FM3-13.4. 2019. *Army Support to Military Deception.* US Department of the Army.

JP3-13.4. 2017. *Military Deception.* US Joint Chiefs of Staff.

McPherson, Denver E. 2010. "Deception Recognition: Rethinking the Operational Commander's Approach." https://apps.dtic.mil/sti/pdfs/ADA535598.pdf.

Moore, David T. 2015. "A Short Primer on Deception and What to Do About It." *American Intelligence Journal, vol. 32, no. 2:* 3-12.

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

Whaley, B. 1969. *Stratagem: Deception and Surprise in War.* Center for International Studies, Massachusetts Institute of Technology.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY
https://buletinul.unap.ro/index.php/en/

New technologies and their impact in the military field

Col. Prof. Cristian-Octavian STANCIU, Ph.D.*
Silviu-Iulian GIMIGA, Ph.D. Candidate**

*"Carol I" National Defence University, Bucharest, Romania
e-mail: cristianstanciu73@yahoo.com

**"Carol I" National Defence University, Bucharest, Romania
e-mail: gymyro@yahoo.com, gimiga.silviu@forter.ro

Abstract

Military geniuses like Hannibal, Caesar, Suvorov or Napoleon proved to the whole world how relatively small armies prevailed through complex battle strategies, ingenuity and courage, through scientific and military knowledge that can make a difference. The technological progress made in the last hundreds of years, based on technical-scientific discoveries, has led the armed struggle to such a high level that technological supremacy, the ratio of forces and military technique are extremely important in the assumption of a military conflict. However, combining conventional resources of combat with modern ones, the use of combined forms and methods of combat, are still issues of general interest, which require adaptable strategies and not least the ingenuity, flair and exuberance of leaders. The impact of new technologies on the military field still remains a dilemma that will probably never be clarified, precisely because of the constant challenges, which are increasingly complex and different.

Keywords:
science; technology; technological progress; robots; balance of power; new technologies.

https://doi.org/10.53477/2284-9378-23-27

Introduction

Approaching a subject based on the impact of new technologies on the military field is extremely sensitive due to the multitude of news, TV shows, permanent technical-scientific discoveries and the fulminant evolution of electronic products around the world. In order to highlight some elements that are necessary for national defense, it is interesting to go through a brief evaluation and interpretation of the effects of technological progress on modern military conflicts and an approach to the relationship between technology and society.

In an ever more complex and volatile security environment, shaping the future serves as a compelling motive for each of us to employ our capabilities in making predictions and forecasts. Drawing on modern technologies, these endeavors aim to enhance the quality of human life and ensure the necessary safety to enjoy it under optimal conditions. Given the overwhelming volume of information, our minds are incapable of processing it all. Consequently, scientists have explored and continue to seek technical solutions that enable the discovery of products capable of significantly simplifying and lengthening our lives.

The continuous technological evolution creates great differences between the nations of the world, precisely because of their different economic power, and our country considering the geostrategic situation in which we find ourselves, tries to keep the stability and predictability regarding the order and security in the area. Romania has been the beneficiary of NATO's political and military objectives since 2004, and this fact has so far ensured the peace and security longed for by entire generations of our population. It is necessary to be aware of the importance of this treaty and to keep up with the partners of the Alliance by maintaining and increasing the interoperability of armaments, techniques and technologies of the military field, by organizing the national territory, thoroughly examining the possibilities of developing our own defense industry and by preparing for a possible war, considering all the political, military, economic, social, infrastructure and information reconfiguration needs. Perhaps one of the most important problems to solve now, in our society, is to make the best decisions regarding the acquisition of the latest techniques and technologies or the attempt to modernize the existing ones. Opinions are still divided, perhaps time and geopolitical challenges will make a difference, but it is clear that we must act in a way that is beneficial to national interests.

Strategic partners of the United States of America and members of the NATO Alliance are developing various strategies to try to achieve faster interoperability goals, by encouraging private companies to produce emerging technologies for the military or by creating acquisitions departments to find better contract-making solutions, because a colossus like NATO cannot and should not be affected by declarations, intentions or, even worse, real attacks on any allied members. In order to achieve the proposed objectives, the Romanian Armed Forces must identify the

military capabilities that need to be improved and especially those necessary to accomplish the interoperability standards in relation to technological evolution and future predictions.

The progress of science and technology is evident and causes the adaptation of existing military art and doctrines, manuals and operating procedures. Emerging technologies such as quantum, artificial intelligence, and robotics can influence weapon systems and combat techniques, communication, computer or detection systems, and can bring fundamental changes in modern military thinking. If the relationship between technology and society is a positive and productive one based on necessity, trust, awareness and efficiency, the military can benefit from the advantages of technological evolution by gaining credibility, respect and fighting power.

By trying to predict the concept of technology development, we will analyze the impact of technological progress on the military field, by studying the effect produced by emerging and disruptive technologies, and the relationship between them and society, trying to include in this limited space some ideas that will attract reader's attention.

Technological progress – the paradigm of the present

The current conflicts are different from those of the past, due to the complexity of the political, military, economic, religious, social, infrastructure, and information issues, due to the precise anticipation of the transformation of the possibility into certainty, especially when the armed aggression comes from two or even three courses of action. We sometimes wonder how it is possible that for centuries the whole world has been influenced by misunderstandings that, most of the time, turned into particularly bloody conflicts.

The struggle for supremacy has led civilian and military leaders to invest huge financial funds in the creation of new, emerging, and disruptive technologies that will surprise possible adversaries, with their use, attaining important benefits to those who possess them, as well as involving huge human and material costs to those who have not kept up with technologies. Now, the EU and NATO have established common directions of action for the faster integration of emerging and disruptive technologies in the military field, trying through the *EU Strategic Compass* and the *NATO Strategic Concept* to issue recommendations to the member states, so that urgent action procedures are started for the research, the production and procurement of intelligent, compatible weapons with common characteristics that allow them to be used jointly by each allied military (Foggo, et al. 2022).

Technological evolution is a result of the interpenetration of science and technology through the use of scientific discoveries in technological processes, the context

in which human civilization and culture developed. In order to understand the current technological progress, we have deduced that it has as its features precisely these components: science and technology, the approach of which always leads to philosophy. Philosophy of technology is a relatively new field, emerging two centuries ago, concerned with the impact of technology on society. In 1994, Carl Mitcham, a philosopher of engineering and technology, defined this philosophy as one of the *"technological humanities"* (The Competitiveness of Nations in a Global Knowledge – Based Economy 2004) because it deals with social science and the humanities, while also being a continuation of the philosophy of science.

Technology encompasses various definitions provided by cultural and scientific experts. In contemporary terms, it primarily refers to the knowledge and application of well-planned, efficient, and practical actions facilitated by machines within companies or institutions. Ernst Kapp, German philosopher and geographer, considered the creator of technological philosophy, published in 1977 the book "Grundlienen einer Philosophie der Technik" in which he states that *"technology is an extension of the human organs, especially the hand, as the archetype of all artifacts, a means of cultural, moral and intellectual progress"* (Mureşan, et al. 1995, 9). Later, other famous philosophers such as James Kern Feinbleman, John Standeumaier, Mihai Drăgănescu, and others analyzed and developed the technology-philosophy relationship and stated that technology had an essential role in human culture, but everything belonging to philosophy should not be neglected, either. Thus, we can say that technology is also science and the scientific method is applied in technology as in science. Science and technology have developed increasingly sophisticated technologies that combined with the philosophy of knowledge and the art of war decisively influence decision-making.

Technological progress can be explained and stimulated, especially towards increasing efficiency, the discovery of modern, cheap, compatible energy sources and especially towards the minimization of stress and hard work, and in the military field of human losses. Preparing for war involves organization, careful examination of land, air or naval combat equipment, personnel selection, execution of a rigorous planning process through the correct assessment of the planimetric details of the terrain in the likely area of operations, and last but not least, technologies compatible with those of allies or that respond to challenges with the same force. Also, knowledge of world politics, enemy movements, troop training, thorough knowledge of subunit and unit commanders, potential soldiers, deceiving the enemy about future intentions are very important aspects of achieving success. So, technological evolution provides military power to a state and the activities preceding the preparation of a conflict can represent the key to the success of a military operation.

The military power of a state is in close correlation with technical-scientific progress; that is why the role of technology in wars is crucial. The military field is facing a strong wave of technological revolutions due to the rapid evolution of mechanisms,

equipment, techniques and procedures that must be maintained at a high level of development. Robotization, computerization, and digitization manifest in all areas of social life and implicitly in the existing armaments and techniques used in present and future conflicts. Military power is *"the military action capability of a state, ensured by its military potential"* and is composed of the budget, infrastructure, personnel, armaments, logistics, defense industry, and research institutions and has as a result the objective of development, the defense of the national territory (Zamfir and Vlăsceanu 1998, 481). National defense is closely correlated with the development of technology and science, with current military thinking paying special attention to military scientific potential, its links to *scientific potential*, and *military potential* for war.

What is military *scientific potential? "A state's possibilities of operative and efficient use of the achievements of science in solving the problems that the strengthening of its defense power entails and is characterized by the following indicators: information assurance, technical-material base, personnel assurance."* (Mureşan, et al. 1995, 44). *Scientific potential* represents the ability to solve the problems of scientific and technical development faced by society or a certain scientific system. The close connection between them is given precisely by the nature of their application and represents the way in which the defense capacity of the country is developed.

The military war potential of a state is a concept of modern war, it represents Romania's defense capacity and is represented by *"the military forces, the materials, the technique and the armament with which the military forces are endowed; material stocks; trained reserves; armaments and combat equipment factories and plants; the system of fortifications; communication channels; geographical situation, and so on"* (Prisăcaru 2021, 131).

The interaction between science and the military domain, the scientific and military potential of war, is dependent on the level of science. Scientific development has always exceeded the possibilities of the military field, but the knowledge obtained through science was used later. For example, the construction of military equipment has always been inspired by the surrounding nature. Bionics implements compact, effective and reliable principles and mechanisms of self-regulation, orientation in space, self-organization, shape recognition, thermal regulation, etc. which are also found in beings. The structure of technical systems tries to copy the patterns of biological systems.

We have inherited little knowledge from human history because the technology that could record and store information appeared several decades ago. Economic growth has determined that, currently, the technical means represented by sets of optical, electronic, mechanical and electrical systems, for recording, storing and transmitting information, are evolving at an overwhelming speed and have unlimited capabilities. Modern technologies in science and technology, such as quantum computers, eliminate empirical methods and give high value to abstract

models capable of issuing strategic, operational and tactical reasoning in the military domain (Cîrciumaru, et al. 2021, 62-63). Quantum technologies, although at the beginning, are in continuous development and aim to achieve complex applications in computing, detection, and communication systems. Quantum computers have *"significant uses in computational fields such as decision-making, process optimization, artificial intelligence, simulation and analysis of natural phenomena, the creation of vaccines and drugs, or the mathematically important factorization of large numbers, to ensure the secure transmission of data"* (Cîrciumaru, et al. 2021, 59).

Artificial intelligence represented by *"the ability of systems or machines to imitate human intelligence as faithfully as possible, can be software systems (virtual assistants, search engines, facial and voice recognition systems as well as image analysis programs) or embedded (robots, drones, autonomous cars and the internet of robots"* (Colorful.hr 2021). The military domain already includes equipment, technique, and weaponry endowed with such capabilities, with use in military medicine, training and simulations, autonomous weapon systems, equipment used for surveillance, monitoring, ensuring information security, electronic warfare, intervention in the neutralization of improvised electronic devices an so on (Georgopoulos and Nurkin 2020, 4).

In the field of operation planning, military action and logistics, digitization and robotics are in full development. If at the beginning of the 20th century, robots were massive, they were built with great financial and intellectual efforts, being programmed only to answer a few questions asked by the builder or to perform simple operations, nowadays they can perform tasks such as: directing traffic, reading books, providing feeding services, serving, cleaning, planning or recalling necessary data and information, moving heavy weights, controlling and timing different issues. The military field benefits from the development of robotics by replacing the human factor in certain structures with a high degree of danger, examples in this sense being the nuclear field where robots are viewed with great interest, the repairing of railways and roads, the guarding of important, strategic objectives, research areas with radiation, as well as their incorporation into aerial or ground combat reconnaissance vehicles equipped with recording, attack and destruction devices. Thus, the field of robotics remains extremely attractive and open to discoveries to which the future will give the appropriate use.

Technological transformations and rising scientific achievements have determined the development of a relatively new field, cyber defense, carried out in accordance with the evolution of the information environment, which involves *"cyber attacks, hostile/influence actions carried out in the public space, disinformation, spread of fake news/manufactured, etc."* (presidency.ro 2020, 6). The development trends in the field of cyber defense are considerable due to the very low costs compared to a classic action, the implementation of cyber security strategies by allied states, the development of research and technical innovations, the accelerated expansion of

virtual space and the development of specific military defense structures (Pătrașcu 2020, 33-35). Cybersecurity has an extremely important role for the military as it ensures the confidentiality of information and prevents "illegal activities that include the use of digital technologies in cyberspace by protecting critical systems and infrastructures against military and other attacks" (European Court of Auditors 2019, 15).

Romania, as a member of NATO, has established cyber defense structures and developed action plans, in accordance with national rules, which ensure the security of the national and multinational cyber domain in cooperation with allied members (Joint Publication 3-12 2018, IV-24 - IV-26). The recent war, which began in 2021, between Ukraine and the Russian Federation, demonstrated that the physical environment for the conflict has a highly developed component – the informational environment – which is permanently influenced by communications, mass media, IT security, international organizations, public figures and military capabilities, which led to unexpected successes for those who were considered to have less and older technology. Probably, the ongoing conflict will start a new direction of action regarding the development of the cyber component at the level of the NATO Alliance and will determine the rethinking of security standards and action strategies in accordance with new technologies that will also bring new vulnerabilities (Hartwig 2021).

So, science and technology ensure technological progress as a paradigm of the present, the latest technologies having incorporated components of artificial intelligence, robotics, quantum mechanics ensuring the development of the country's military power, by creating a climate of safety and well-being on all social levels. At the moment, each of us is happy and excited about the benefits of technology, but it remains to be seen how it will evolve and what the impact on human life in general and in the military field, in particular, is going to be.

The influence of technological development on the field of defense

The accelerated technical-scientific progress represents for the Romanian Army one of the permanent challenges because it is closely related to the human resource that must be prepared, trained, maintained and developed in accordance with the acquisitions. Scientific discoveries were tested most of the time with priority in the military field, which led society to rigorously select human values, which are to use new technologies in military activities.

There is a mentality fueled by the present information, whereby the highly developed states believe that without technology the war is almost impossible to sustain and is lost, right from the start. Some conflicts, such as those in Iraq, Afghanistan, and the

https://doi.org/10.53477/2284-9378-23-27

Balkans, have shown that technological supremacy allows the rapid destruction of the enemy without significant organic losses. It is time, therefore, to realize that the impact of technical-scientific development on the military field can be radical and must be oriented towards development.

What directions of action are necessary to achieve technological interoperability in the armies of NATO members? We believe that in order to faster achieve optimal cooperation between the existing equipment, technique and technologies in the armies of the NATO allies, it is necessary to increase the importance of institutions with attributions in the field of education, research, production of military equipment, and technologies, participation in conferences, equipment exhibitions, materials and technique, organized at the national and international level, as well as the realization of plans for the improvement of armaments, based on rigorous planning, the increase of cooperation with the armies that already use modern equipment, the development of communication and information systems and so on.

Within the Ministry of National Defense there are institutions that are permanently concerned with the achievement of the technical and technological dimension, such as the Defense Staff, the Research Agency for Military Equipment and Technologies, the General Directorate of Armaments, the Joint Logistics Command, which delegates experienced military personnel, to participate in meetings, working groups, analysis sessions with representatives of the defense industry in the country and abroad. Based on the reports drawn up following the implementation of such activities, the need to adapt the equipment and armaments to the realities of the modern battlefield emerges more and more. However, it is difficult to harmonize costs with efficiency and the need to renew equipment and techniques. Many times, the needs are much greater than the budget, therefore it is necessary to have an *iron will* to justify the benefits achieved. The programs for the acquisition and modernization of Romanian military equipment are viable, necessary, and follow their course of action according to planning, but the threats present in the world prevent in some cases the delivery or production on a larger scale of some equipment or technical elements imperatively necessary for the current development.

Having a strong military requires effective leadership, which requires a quality planning and decision-making process. This activity involves the improvement of communication, mainly IT, and the purchase of equipment and software programs to support this complex and dynamic process.
Do we therefore have strategies that make technical and technological, operational performance with those of the Alliance? We could say yes, because, at this moment, soldiers from the Alliance, who have been stationed or are training on the Romanian territory, appreciate the efforts made to achieve an effective defense position on NATO's eastern flank, by providing equipment comparable to their own, in joint exercises, by ensuring cooperation and communication between structures, and last but not least by good fighting skills.

Do we need technological superiority in the event of military conflicts? Given the current geostrategic situation, we believe that now is the time when we can adapt command structures to the information age, we have the opportunity to develop infrastructure networks and cyber defense equipment, we can increase investments in emerging and disruptive technologies, or we can cooperate with the private sector to develop its own production of armaments, techniques, and technologies (NATO 2022, 7). Therefore, it is possible and necessary to continue equipping the military with new technologies to meet threats and fulfill our obligations within the Alliance. Currently, we can state that in order to ensure technological supremacy, we have solutions to support it through the existing procurement programs, and through membership in NATO and the EU, we can access programs for the absorption of development funds in many directions necessary for national defense.

The technical-scientific development and the impact of the procurement of new technologies require, on the other hand, high-quality personnel that is properly prepared and trained to be able to face the challenges given by modern technology. Analyzing the military history of the Romanians, we found that in most important battles the ratio of forces was almost always inferior to the various enemies, but voivodes, commanders, and military leaders created strategies that tipped the balance of power towards balance, by setting up trained military structures, achieving surprise, the progressive engagement of resources, ensuring the effectiveness of the means of combat available, the use of the physical space for carrying out operations for one's own benefit, as well as influencing the morale of the enemies. At the same time, increasing the cohesion of their own troops in battle was the main weapon of the Romanians, being developed by the commanders by knowing the subordinate personnel down to the smallest details and training them to use the technique to the maximum extent possible. Analyzing these lessons learned, the Romanian military art was eventually developed.

The ratio of forces has a decisive role in a military conflict, but it does not always ensure the chance of success, sometimes the exaggerated arrogance of commanders or the ineptitude of planners regarding the use of means in battle leads to true defiance of the objective laws of armed conflict (Eminescu 1986). Thus, we consider that the ratio of forces and means is an important factor in the planning and conduct of military conflicts, but it is not a decisive one, because the intelligence, training, and, most of all, the motivation of the combatants can be the key to success.
We appreciate that the lessons learned from the tumultuous history of the Romanians and the impact of the continuous development of technology in the military field, converge towards several directions of analysis depending on the level at which planning and decision-making are performed.

At the strategic level, a direction of action could be the creation of small combat groups, thought on concrete objectives, made up of soldiers with skills trained and developed towards the level of perfection in the use of sophisticated weapons, the

https://doi.org/10.53477/2284-9378-23-27

quality of the concept of strategic action, the ability to plan and lead the command-control system and the provision of the strategic logistic reserve.

At the operative and tactical level, situations change depending on the physiognomy of operations, the quality of the human resource, and the technique used intelligently. The concept of operations carried out at the operational level must include maneuver schemes that aim to maximize the quality of the execution of actions, the adoption of the most ingenious forms of combat and the provision of the best conditions for surprising the enemy.

At the tactical level, small force groups capable of executing complex missions in difficult situations are the task of commanders. They are appointed, as a rule, to find solutions for training the military regarding the knowledge and use of armaments and techniques, in the smallest details and most importantly, in search of ways to motivate them, in line with expectations.

Analyzing the conflict between Russia and Ukraine, which began in 2021, it appears that, in most situations, the Ukrainian Army has coped, so far, primarily due to its knowledge of the terrain, both in the open field, and especially in urban battles. It also turned out that one of the most important factors in achieving resilience so far has been the judicious blending of all combat methods and procedures. Continuously launched surprise actions, physical and psychological influence, the creation of intermediate and reserve phase lines, the misleading actions, they all created major surprises at the tactical, operative and even at strategic level. Be that as it may, the not yet concluded conflict demonstrates the competition of military technologies used and Ukraine's effort to resist a much larger force.

The impact of scientific development on the Romanian military field is real and radical, the acquisition of cutting-edge techniques and technologies being imperatively necessary, simultaneously with the attempt to modernize and revitalize the Romanian defense industry. The need to modernize the technique is extremely obvious and it has been shown that it radically influences the fate of military conflicts, both through the effects of digitization, automation, robotics and the introduction of artificial intelligence on certain components of military technique and through the effects obtained through the means of communications and IT that ensure security cyber of the entire national defense system.

Conclusions

It is complicated to answer all the questions related to the effects of technology on the conduct of current, modern military conflicts, but trying to do it, in part, to the topics that appear daily in the contemporary press, is an important step in creating conclusions and measures that need to be adopted. As mentioned above,

technological transformations significantly influence the military field, in terms of weaponry, communications, intelligence, surveillance, monitoring, and control of the military operations. The combat power of a state is given by the introduction and increase in the number of weapon systems and advanced technologies, such as launch systems, missile launchers, and combat systems. Communications and information are the key elements of maintaining the link between military structures and can only be achieved through high-performance communications and IT systems, which radically support the planning and decision-making process as well.
From the analysis of the science-technique-power relationship, it is clear that the first factor is the prerogative of scientists and is the basis of useful discoveries and innovations. Military educational institutions such as the „Ferdinand I" Military Technical Academy train engineer officers who analyze the needs of the defense system and cooperate with research institutions for the coordinated realization of modernization and ensuring a state of safety regarding the technologies used in military operations.

We appreciate that equipment is the key factor in achieving troop mobility, therefore the accelerated pace at which the automotive field develops and the environmental protection measures taken worldwide lead the army to establish clear and honest objectives and levels of ambition, through the National Defense Strategy of Romania and the Military Strategy of Romania. Romania's scientific and military potential is immense and refers to the ability to use and eventually produce weaponry and advanced technologies to fulfill our political, economic, and military objectives. Investing in research and development, improving infrastructure, ensuring adequate education and training of military personnel, and investing in advanced technologies and modern weaponry are necessary measures to improve military potential.

The new concept that is increasingly present in our lives – artificial intelligence – is already implemented, by adapting existing technologies, and by introducing learning algorithms that make possible operations that in the past required a lot of well-trained human resources. In order to be interoperable with the equipment of NATO member armies, we must be part of joint projects and accept that partnerships are the key to success. By reading and understanding the new concepts of international military organizations we can appreciate what it means to use an effective leadership system, to have a quality planning and decision-making process, and to estimate the effects of a nation's technological superiority.

Analyzing the history of the last world conflicts in which Romania participated, it is clear that the army did not succeed in equipping it with modern equipment prior to military actions, relying more on the loyalty of its neighbors and the validity of the treaties and agreements concluded. Thus we entered the First World War unprepared, not knowing the real situation of training and equipping the army with technologies comparable to the time. World War II surprised us with the same problems that turned into disasters and huge human and material losses. It remains to be seen if

we will manage to integrate, to reach the levels of ambition set by Romania's Military Strategy and if we will have the political ability we have shown so far, to smooth out possible future conflicts.

Following current military conflicts, it is difficult to estimate what future ones will be like, but it is not useless to try to predict them, in order to have reasons not to give up on development. Probably many of us do not imagine how it is possible that in the 21st century we still need armaments through the development of new technologies and experiences, which have produced huge destruction over time. The contemporary reality, however, proves to us that it is necessary to approach technological progress with an openness to the military field, and Romania, through the military leadership structures, should have a courageous approach to the future, by realizing strategies for the development of technique and technologies, such as the Program of transformation of the Romanian Armed Forces until 2040, with clear deadlines and responsibilities and having adequate financial support to maintain the objectives.

References

Cîrciumaru, F., D.L. Petrescu, C. Băhnăreanu, M. Zodian, C.C. Ioniță, G. Stoenescu, and M.T. Potârniche. 2021. *The impact of new technology on military art.* Bucharest: "Carol I" National Defence University Publishing House.

Colorful.hr. 2021. „Ce este Inteligența Artificială – cum funcționează, tipuri, aplicabilitate pe piața muncii. https://www.colorful.hr/ce-este-inteligenta-artificiala-cum-functioneaza-tipuri-aplicabilitate-pe-piata-muncii/?utm_term=&utm_campaign=NNC+%7C+Search+%7C+Dynamic+%232&utm_source=adwords&utm_medium=ppc&hsa_acc=9670787410&hsa_cam=17455092683&hsa_grp=1375498.

Eminescu, Gheorghe. 1986. *Napoleon Bonaparte.* Bucharest: Romanian Academy Publishing House.

European Court of Auditors. 2019. "Challenges for an effective UE cybersecurity policy." https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_RO.pdf.

Foggo, James, Nicholas Nelson, Joanna Van Der Merwe, and Nico Luzum. 2022. "Elevating Our Edge: A Path to Integrating Emerging and Disruptive Technologies." https://cepa.org/comprehensive-reports/elevating-our-edge-a-path-to-integrating-emerging-and-disruptive-technologies/.

Georgopoulos, Giorgos, and Tate Nurkin. 2020. "The current state of AI in defence and security." https://www.defenceiq.com/defence-technology/whitepapers/the-current-state-of-ai-in-defence-and-security.

Hartwig, Ben. 2021. "Lessons learned: Cybersecurity in the defense industry." https://www.defenceiq.com/air-land-and-sea-defence-services/case-studies/lessons-learned-cybersecurity-in-the-defense-industry.

Joint Publication 3-12. 2018. "Cyberspace Operations." Joint Chiefs of Staff, US Army. https://irp.fas.org/doddir/dod/jp3_12.pdf.

Ministry of National Defence. 2021. "Military Strategy of Romania." https://www.mapn.ro/legislatie/documente/STRATEGIA-MILITARA-A-ROMANIEI-ENG.pdf.

MSpoweruser.com. fără an. *IBM bate Microsoft la acuratețea recunoașterii vorbirii.* Accessed 6 January 2023. https://mspoweruser.com/ro/ibm-beats-microsoft-speech-recognition-accuracy/.

Mureșan, Mircea, Gheorghe Ilie, Vasile Grad, and Alexandru Mihalcea. 1995. *Advanced technology and the military field.* Bucharest: Military Publishing House.

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

NATO. 2021. "NATO Advisory Group of Emerging and Disruptive Technologies." Annual Report. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/7/pdf/220715-EDT-adv-grp-annual-report-2021.pdf.

Pătrașcu, Petrișor. 2020. "Risk and uncertainty in cyberspace." *Bulletin of "Carol I" National Defence University* vol.5 (nr.4).

presidency.ro. 2020. "The National Defence Strategy of the country for the period 2020-2024." https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf.

Prisăcaru, Dan. 2021. *In the outpost of the fight for survival.* Bucharest: Military Publishing House.

Zamfir, Cătălin, and Lazăr Vlăsceanu. 1998. "Dictionary of sociology." Bucharest: Babel Publishing House.

No.2/2023, APRIL-JUNE
https://doi.org/10.53477/2284-9378-23-28

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

The physiognomy of modern multinational joint operations and the manifestation of mobility in contemporary warfare

Rodica-Cristina BĂLAN-LISEANU, Ph.D.*

*"Carol I" National Defence University, Bucharest, Romania
e-mail: rodica.liseanu@yahoo.com

Abstract

Recent conflicts at the international level highlight the joint and multinational character of multinational operations in today's security environment where conventional and unconventional, asymmetric actions are combined. Over time, in order to optimise and make more efficient the human, information and material resources employed, and to ensure a flexible and pragmatic strategic vision, there has been a continuous need to seek proactive, collective involvement, both from a decision-making and an operational perspective. Thus, there emerged a pressing need for modernisation in the architecture of multinational joint operations. It applies the vision of a qualitative analysis of the global order in the context of great powers, emerging powers and international organisations whose effectiveness is questioned. At the same time, this article analyses the dynamics of contemporary multinational interventions and explores their options for manifestation as autonomous or assembled.

Keywords:
joint operations; multinational operations; current security environment; hybrid warfare; international organizations; modernization.

The melting pot of the international security system is a mixture of national security interests, values and objectives, and external challenges.
The physiognomy of the modern operating environment is becoming increasingly clear, the evolution of the armed conflicts of the future is imminent and accelerating, and the armed forces are increasingly characterized by versatility, mobility, interoperability, adaptability, flexibility, availability, diversity, and speed. Mass warfare is being replaced by hybrid warfare (conventional and unconventional). A revolution is taking place in the military in terms of information, ideology, operations, strategy, and force policy in general.

Artificial Intelligence contributes to some of the greatest strengths of modern warfare through its initiative, speed, multidimensionality, ubiquity, and convergence. Information warfare is fierce, with automation and digitization impacting the infrastructural, cultural and military, diplomatic, political and socio-economic domains.

From a methodological perspective, this article aims to develop, through the analysis carried out, a process of prefiguring possible solutions to current problems in the international security system. Through observation, description and explanation, the general framework, the social actors involved and their mission are outlined. The procedures of content analysis ensure increased objectivity and a systematic approach. They also prioritize anteriority, enhancing the feasibility of deriving a certain type of connection within this unique pattern of anticipation. Through the practice of triangulation, the veracity of information from a multitude of different sources is verified, the case study being one of them.

The modern, innovative multinational, joint operations are placed between Maslow's Pyramid, in its upper zone of the need for self-actualization, and Bloom's Taxonomy, in its exhaustive approach. Cognitive processes that underpin multinational joint operations evolve from information recognition, definition, repetition and reproduction to understanding, application, analysis, value judgments through evaluation, and are completed through creation. Innovation is built on imagination, planning and the generation of content of interest with significant value added in the security and defence sphere.

The article materializes an articulated vision between theory and practice, between armament in different generations of war and disarmament, stability and peace support, evolving from concepts, purpose, principles, characteristics, advantages and challenges of multinational operations in the context of security and defence modernisation. The proposed qualitative analysis is chosen in the logic of discovering elements of novelty. Starting from the society of the present and continuing with that of the future, it circumscribes a time of information, innovation and creativity.

1. Multinational operations. Conceptual references, classification, principles

Multinational joint operations are military actions of varying scale and size, carried out with groups of army forces, within coalitions and alliances, under single political control and command and with a single objective (Frunzeti 2000, 23). Multinational operations are those military actions involving two or more countries. The first is the simple combination of forces, so countries join together militarily to merge their separate military forces into a single, stronger force. They also serve a political purpose, as the combined efforts of two or more countries give legitimacy to action by demonstrating broad international approval of the operation.

Multinational joint operations are conducted both in war and in peacetime as part of stability and support operations. Military stability and support operations encompass a wide range of activities and actions aimed at achieving a variety of objectives, including the fulfilment of national interests, deterrence and prevention of war, promotion or, as appropriate, restoration of peace, reduction of tension between states below the level of armed conflict and resolution of international crises, and support to civilian authorities in dealing with internal crises.

In their content, military stability and support operations may include elements of both combat and non-combat operations conducted in peacetime, crisis and war (Frunzeti 2000, 23). In other words, there will be numerous situations that, due to their nature, will exhibit war-like characteristics, including combat actions utilizing military capabilities to achieve specific objectives.

Stability and support operations contribute to the achievement of the strategic national security objectives of the states that organise them, and sometimes also to international security objectives. In peacetime, the primary mission of armed forces is to ensure deterrence of all types of aggression, i.e. both external and internal aggressive actions and combined actions.

We therefore consider it appropriate to use the term *multinational joint stability and support operations* for the following reasons:

- the impossibility of establishing the exact dividing line between war and military stability and support actions;
- the participation under a UN or OSCE mandate of several States in the resolution or management of crisis situations;
- the content of operations is correlated with the need to belong to stability or peace support.

For a correct understanding of the terms used we will briefly define the terms *alliance* and *coalition*.

Alliance is "*an arrangement made on the basis of formal agreements between two or more states, with medium and long-term political and military objectives, which*

aims to achieve common interests and goals and to promote the national values of its members". (Ministry of National Defence 2001, 12)
Coalition, as opposed to Alliance, "*is an ad hoc political and military commitment between two or more states to carry out joint actions*". (Ministry of National Defence 2001, 12)

Within the Alliance, exceptionally, a lead nation may be designated - where all Alliance members subordinate forces to a single nation by transfer of authority, or a joint staff command is formed to exercise control over both multinational and national units. Multinational actions within the coalition take place outside the Alliance's established links, usually for one-off situations or for long-term cooperation in a specific, narrowly defined area of common interest. As in the case of the Alliance (for conjectural situations), a lead nation may be established, based in particular on criteria relating to the extent of participation with combat, logistic and information forces and assets in planned operations.

Command structure of multinational forces:
a) Alliances are characterized by years of cooperation between nations.
In alliances, common objectives are agreed upon: standard operating procedures are established, appropriate plans have been developed and exercised between participants, i.e. there is an organisational plan, interoperability between equipment, and command relationships have been firmly established.
Alliances are normally organised under an integrated command structure, which provides unity of command within a multinational framework. Key elements in a command structure are that a single commander will be appointed, that his staff will be composed of representatives of all member nations and that all subordinate units and their staffs will be integrated down to the lowest echelon to accomplish the mission.

b) Coalitions are normally formed as a rapid response to an unforeseen crisis.
In the early stages of such an emergency, nations rely on military command systems to control the activities of their forces. Initially, therefore, the coalition will involve a parallel command structure.
As the coalition evolves, coalition members may choose to centralise their efforts by nominating a lead nation to receive command of the coalition. In this type of coalition, all coalition members subordinate themselves to a single partner, generally the nation that provides the predominant number of resources and personnel. However, subordinate nations' commands maintain their national integrity. The command of the leading nation establishes integrated staff sections, with a composition determined by coalition leadership.
The principles of multinational operations are Unity of effort/goal, Sustainment, Concentration of effort, Economy of effort, Flexibility, Definition of objectives, Initiative, Maintenance of morale, Surprise of adversary, Avoidance of surprise, and Simplicity (Ministry of National Defence 2001, 12).

2. Architecture of multinational joint operations. Characteristics, advantages, and challenges

From micro to macro, an operation is a military action or the accomplishment of a strategic, tactical, assurance, and training military mission, the process of continuing combat including movement, supply, attack, defense, and maneuver necessary to achieve the objectives of any battle or campaign. Multi-nationality, on the other hand, is a reality at the operational level, as it reflects the Alliance's political need for international consensus and legitimacy for military action. Multi-nationality has become the standard for conducting missions around the world, and today we see more and more nations willing to pool their resources to promote global peace and stability (Ministry of National Defence 2001, 12).

When we talk about joint multinational operations, we refer to the totality of land, air, and sea actions carried out by a group consisting of forces or elements and assets belonging to several categories of military forces, with military forces of different sizes in the corresponding environment specific to each of them, in a determined geographical area, in a unitary concept and under a single command, exercised by a gathered operational command, under political control in order to achieve some strategic objectives. (Ministry of National Defence 2001, 12).

A more comprehensive definition of the joint operation stipulates that, within it, the effort focuses on synchronizing the forces and capabilities provided by the "land, naval, air, space, cyberspace, special operations and other functional forces" components, one of which being able to predominate at a certain stage of the operation. Under these conditions, the actions carried out assume the integrated and united involvement of all categories of forces that intersect, overlap, complement and inter-condition each other dimensionally, informationally and operationally. (Ministry of National Defence 2012, 136)

NATO must always be prepared to work with traditional members and partners, but also with other, less familiar forces – in coalitions. Mutual trust is essential when working in a multinational environment (NATO 2012).

Within NATO, *Multinational Combined Joint Operations* are those operations in which armed forces from two or more countries participate and which involve at least two categories of forces. The concept of *Allied Joint Operation* refers to operations in which forces from only NATO member countries participate.

In NATO Doctrine, multinational military operations conducted in wartime are considered multinational joint operations for collective defence under Article 5 of the North Atlantic Treaty, and those conducted in peacetime are considered UN/ OSCE peace support operations conducted directly by the UN/ OSCE together with non-Article 5 crisis response operations conducted by NATO under a UN/ OSCE mandate (NATO 2012).

The fundamental purpose of a multinational operation is to direct the military effort to achieve a common objective. Multinational operations are unique. Each national commander is responsible to the multinational force commander. The joint operation is executed within a defined period of time, within the physical boundaries of a geographical area (called a Joint Operation Area - JOA), where the joint force commander plans and executes a mission. "*The military structures of the future will be designed and trained to carry out complex military actions, in a joint context, with a multinational, modular structure that can be adapted at short notice to the mission and to the specific conditions of deployment*" (Mureşan 2005, 46).

In terms of characteristics, in addition to the existence of groups of two or more categories of forces (land, air, sea), we also find: action in a well-defined geographical area, the existence of a unitary concept, exercising a single command, aimed at achieving strategic objectives and commanded by a joint operational command. The integrated nature of military action is a feature of operations, the emergence of which has been brought about by the multiplication of the action couplings that make it up, and is a natural consequence of the increase in the number of types of weapons and the organisation of the modern army into categories of army forces.

3. Perspectives of modernity on multinational joint operations

3.1. Generations of war on the time axis

Modern warfare has evolved generationally. It is believed that the strategic and tactical advantage will go to the one who is proactive, the first to transition to a new generation, the one who understands change and adapts in the shortest time. In contrast, a nation that is slow to adapt or not open to change will lose its advantage. From one generation to the next, there has been a steady increase in battlefield dispersion and a decrease in reliance on logistics.

The first generation of warfare (1648-1850) involved large numbers of troops, linear tactics (line or column tactics), predictability, and low readiness of enlisted troops. Technique and weaponry were rudimentary (the smoothbore musket), operational art was conceptually non-existent, but was practiced in isolated cases by an illustrious commander such as Napoleon.

The second generation of warfare (1850-1918) was characterised by the perfection of weapons, the means of combat, and the increase in firepower. War industries (artillery, bombardment aircraft), repeating fire weapons, and tactics remain linear, but a large volume of fire can be executed. Resources improved with machine guns, barbed wire, indirect fire, and movement, still remain linear. Means of fire are carefully planned with a view to hitting an objective, and defence is by direct contact (Lind, Schmitt and Wilson 1989, 22-26).

The third generation of warfare (1918-1990) involves the increased mobility of forces, manoeuvre is given greater importance in the battle space, across the spectrum of military action, blitzkrieg attacks, tanks, and non-linear tactics whereby the opponent is surprised by envelopment, reversals, infiltration. The defence is based on counter-attack, takes place in depth, and static actions are replaced by rapid actions (Petrescu 2021). Mobility makes the transition from third to fourth generation more visible. Thus, the smaller the troops, the more agile and manoeuvrable they are. Fixed points of communication will be increasingly rare, precisely because of the vulnerability they imply. The lines between responsibility and mission are increasingly blurring, and this will become more and more apparent in the next generation.

The fourth generation of warfare (2003-2011) has manifested itself, particularly after 1990, characterised by a predominance of unconventional forms of combat, non-linear tactics, and technological potential, but also asymmetry as a product of huge technological gaps. The threats present in the future operational environment are hybrid, including, in addition to conventional actions, catastrophic actions – chemical, biological, radiological and nuclear weapons of mass destruction (WMD/ CBRN), disruptive actions such as cyber aggression, information operations, psychological operations, and irregular actions – terrorism, insurgency, guerrilla warfare, piracy, extremism, partisan groups, organised crime, subversive actions (Petrescu 2021).

There is a low possibility of interception of communications, artificial intelligence can radically alter tactics, robotics is evolving at a rapid pace, vehicles can be remotely piloted, and intelligent soldiers armed with state-of-the-art weapons can cover large areas.

The American vision superimposes asymmetry on an '*axis of evil*'[1] with which it associates the proliferation of weapons of mass destruction, terrorism, and the actions of highly technological countries. A distinction is made between confrontations which are the product of chaos and generate chaos, and asymmetric confrontations which oppose forces that are disproportionate in terms of organisation, technology, equipment, or potential (Mureșan and Văduva 2004, 49).

Leadership is a priority in this framework, as it is important to continuously pursue operational and strategic objectives, to be able to concentrate, select targets, manage challenges, supervise a constantly changing environment, manage and manipulate the excess of information, without losing sight of the essential content, i.e. those with value potential.

Forces participating in the armed conflicts of the future will be further developed through surgically precise strike systems, electronic and

[1] The emblematic metaphorical concept of the George W. Bush era, which became an essential pillar of the foreign policy architecture, referred to the major threats to the US - Iran, Iraq and North Korea, to which Syria, Libya and Cuba were later added. In the same key, there is the concept of the Troika of Tyranny describing the authoritarian, dictatorial Latin American triad of three enemies of democracy – Cuba, Nicaragua and Venezuela.

information or psychological warfare. The army is thus shaping up to become a fast-action, mobile, maneuverable, modular and versatile force, proactive, trained and equipped, with a high degree of connectivity to information networks and, above all, self-sustainable through its resilience (Petrescu 2021).

A future generation of warfare is beginning to take shape in terms of the future operational environment, so we could already start to bring to the table the idea of a fifth generation of warfare, a generation of innovation, of digitization, still insufficiently understood and exploited to its true potential. Knowledge and the revolution in thinking continue to serve as inexhaustible sources that facilitate the preparation and construction of unpredictability, non-traditional actions, enhanced precision, and the acquisition of new equipment and installations.

Future warfare as critical infrastructure involves the transition from the brutal form of the use of force to subtle modalities, today's new armies aim to shift from space-oriented to time-oriented, and military doctrines are adapting to increase the ability to project power over long distances, with an emphasis on joint operations between different multinational operations, on synchronized simultaneous attacks, with increased speed, with an emphasis on initiative (Georgescu 2016, 18-19) As Alvin Toffler notes, "*military doctrine continues to change in all the world's militaries*." (Toffler 1996)

3.2. Perspectives of modernity in security and defence

Primary technologies have been around for over 50 years, but with the rapid growth of computing power, major advances have occurred in recent years as a result of more and more new algorithms.

Modernisation has been gradual on several levels. Crisis management or collective defence through alliances is a benchmark in the modernisation process. The North Atlantic Treaty is thus the central international political document governing their establishment, organisation and operation.

Disruptive technology is an innovation that integrates, creates and recreates the lifecycle, in a global and centralized context where investors or consumers are ready to vary different areas such as artificial intelligence, robotics, nanotechnology, autonomous vehicles, machine learning, specific industries and business operations, in the context of the need to fund military operations.

The proactive approach envisages a transition from traditional technologies to high-tech expressions of human societies. Embracing the digital sphere is a lengthy process for ordinary people, but the impact of disruptive technologies is having a strong impact on their mobility, improving the quality of everyday life. The masses need to understand the challenges of excellence, to perceive digital learning as a valid and competitive competitor to traditional patterns. Changing the mindset of this comfortable resistance is the first step to generating sustainable solutions.

Science solves the toughest economic, societal, military, health, and environmental challenges.
Disruptive technologies are the future of technological ecosystems, and their advances will be heralded by revolutionary interventionism in future industries.
In recent years, our planet has changed, with the 21st century marking the emergence of a new industry based solely on information and technological advances.

Throughout its history, in order to keep pace with the new imperatives in the field of security and defence, specialists have progressively worked on Artificial Intelligence and other technical, technological and informational revolutions, having had a purpose, and a vision; thus, they have brought benefits, but also risks. These can be used to develop new algorithms that can perform everything from accurately calculating distances (e.g., the shortest route to work) to forecasting environmental trends, so important in environmental security. At the same time, Artificial Intelligence improves the capabilities of an intelligent vehicle and makes it autonomous. Several applications are used for military and humanitarian purposes. For example, a multi-sensor dispatch robot uses laser technology combined with *intelligent thinking*. These machines are usually personalised, with robots being given funny or human names.

Artificial intelligence is a growing field with implications for national security. Artificial intelligence technologies present unique challenges for military integration, especially since most AI development is taking place in the commercial sector. Development in conjunction with intelligent vehicles can actively contribute to both the private and public sectors. The military already uses autonomous machines, especially flying machines and smart vehicles in so-called "*decoy operations*".
Artificial intelligence strengthens state security through its algorithms that can accurately predict vulnerabilities, risks, and threats. The coalition between autonomous vehicle technology and artificial intelligence aims to improve the efficiency, safety, and performance of military logistics.
There is constant use of Artificial Intelligence in all fields of activity, in security and defence it is imperative, even a priority, thanks to the benefits it brings.

At the global level, there is an accelerated technological advance, with China and the United States remaining the leading states. The benefits of Artificial Intelligence are contained, in the field of internal and external intelligence, through the formulation of the concept of "*augmented intelligence*" which implies an extension, not a replacement of the human intellect (Mocanu 2020).
Artificial Intelligence finds wide applicability by exploiting open sources. OSINT, a predominantly technical discipline, processes large volumes of information material (big data), in radio research - SIGINT operators extract information from signals in the electromagnetic spectrum, the applicability of Artificial Intelligence continues by exploiting human HUMINT resources, as well as by exploiting information from images - IMINT.

Another important area in the representation of Artificial Intelligence in security and defence is the protection of information. Thus, in the broad theme of cyber-security, the risks of compromising the various systems of institutions, companies and organisations are identified.
In the future, violence is going to become dependent on technology (artificial intelligence, optics, drones, satellites, telecommunications, infrared thermal imaging equipment, night vision equipment, state-of-the-art software, digital accessories, detectors, temperature sensors, etc.).

In cyber warfare, advanced hostilities are the result of initiatives characterised by intelligence, inventiveness, adaptability and interconnection, observation, insight and, above all, perseverance.
The modern battlefield is moving from the physical to the virtual, the physiognomy of military action is evolving rapidly, adapting its speed of reaction to current challenges, and the contemporary military phenomenon acts by integrating these connected actions into joint operations.

4. Operation Desert Storm – Case Study

Operation Desert Storm took place on the invasion of Kuwait by Iraqi leader Saddam Hussein on August 2, 1990 (Kaplan 2020, 69). The international community responded accordingly to Hussein's military action and organized itself into a large military coalition led by the US. What made Kuwait so desirable to both Iraq and other international powers was that it offered control over the region's rich oil resources. (Kaplan 2020, 69). The goal of Operation Desert Storm was to liberate Kuwait from Saddam Hussein's troops.

Prior to *Operation Desert Storm* there was *Operation Desert Shield* which consisted of action by American Rapid Reaction Forces. This operation also used ground, air, and naval forces to lead actions in Iraq. The operation ended on 17 January 1991 when Operation Desert Storm began (Encyclopaedia Britannica 2023).

Operation Desert Storm was authorized by UN Security Council Resolution 678 issued on 29 November 1990, which called for the withdrawal of Iraqi troops from Kuwait and a cessation of violence in accordance with previously issued resolutions. The resolution also provides for the use of all necessary means by UN Member States to bring Iraq into compliance with the provisions of the resolution (UNSCR 1990).

On 17 January 1991, *Operation Desert Storm* began with an air action led by 9 AH-64 Apache helicopters, 101st ABN DVN, Air Force MH-53 Pave Low helicopters. Twenty-seven Hellfire missiles were used to target Iraqi radars, followed by 100 Hydra-70 missiles hitting anti-aircraft weapons. These strikes allowed U.S. Air Force F-15E Strike Eagle aircraft, along with EF-111 Ravens, to penetrate Iraqi airspace

without resistance. Together with these, both coalition air and naval missiles were able to hit targets without difficulty (U.S. Army Center of Military History n.d.).

On 24 February, ground action began. The first ground actions included placing intelligence troops on the ground so that they could gather the necessary intelligence and provide it to allied forces. At the same time, ground troops began their assault on Kuwait City and took advantage of the tired and hungry Iraqi troops to disrupt their structure eventually causing them to retreat east. Iraqi resupply and withdrawal routes were also blocked. On 26 February the decisive battle with the Tawakalna Division took place. Allied forces utilized tanks, ground components, Apache helicopters, and air components in the ensuing battles, resulting in numerous successes. Actions at ground level lasted about 100 hours; and together the air and ground actions managed to destroy more than 3000 tanks, 1400 armament carriers and 2200 artillery pieces (U.S. Army Center of Military History n.d.). The air actions lasted 6 weeks, being also the ones with which Operation Desert Storm debuted (Collins 2019).

There were also a series of coalition naval operations in the Persian Gulf designed to protect US Navy aircraft carrying equipment into the theatre of battle, to strike at any Iraqi defensive attempts from the coastal area, to remove potential submarine mines and to prevent possible amphibious attacks by Iraqi forces. (Encyclopaedia Britannica 2023) The air operation targeted Iraqi strategic targets so that the coalition could achieve its political goal as quickly and with as few strikes as possible (Beagle 2001).

Operation Desert Storm ended with the declaration of a ceasefire. The effectiveness of the coalition strikes was noted as, in two days, Iraqi troops lost 185 armed vehicles and 400 trucks carrying ammunition. The success of the mission was based on coalition force training and air-to-ground combat doctrine (doctrine tested during *Operation Desert Storm*). (U.S. Army Center of Military History n.d.)
Following the liberation of Kuwait, humanitarian missions took place to assist refugees, re-establish Kuwait's control over the city, and make arrangements for the distribution of water, food and necessary medical assistance (U.S. Army Center of Military History n.d.).

Underpinning the performance in the operation was the use of new technologies in combat techniques at the time, including hardware that made high-precision strikes possible, Abrams tanks, Apache attack helicopters, Bradley Fighting Vehicles, Black Hawk utility helicopters and the Patriot missile system. Operation Desert Storm is also known as the *First Space War* because it is the first major military operation to use space-based capabilities. *The Global Positioning System* (GPS) was used for ground-level navigation which led to the victory of ground troops after only 4 days. SATCOM satellite communications provided communication between forces on the ground and between forces on the ground and the base, which was

particularly important because there were no communication systems in the areas of operations. *Friendly Force Tracking* provided military decision-makers with very clear information on the situation on the ground, as well as effective command and control capabilities. (U.S. Army Center of Military History n.d.)

The operation also involved close cooperation between forces operating in theatre and the intelligence services. Coalition troops also acted in the psychological realm, through their quick successes they caused Iraqi soldiers to surrender; other actions in the psychological realm consisted of them turning off the electricity causing psychological effects within the opposing troops (Beagle 2001, 54).
In order to successfully achieve the strategic goal of causing the withdrawal of Iraqi forces from Kuwait, Allied forces carried out actions consisting of imposing air superiority, destroying strategic targets, and striking Iraqi ground targets. These were successfully accomplished by coalition forces (Encyclopaedia Britannica 2023).

Operation Desert Storm was conducted under the leadership of the US, with 35 states participating in the coalition of forces: Afghanistan, Argentina, Australia, Bahrain, Bangladesh, Belgium, Canada, Denmark, Egypt, and France. Germany, Greece, Hungary, Honduras, Italy, Kuwait, Morocco, Netherlands, Niger, Norway, New Zealand, Oman, Pakistan, Poland, Portugal, Qatar, Saudi Arabia, Senegal, USSR, Spain, Syria, Turkey, United Arab Emirates, United Kingdom (Englehardt 1991). Each of these forces contributed a different number of troops and military equipment, with the largest contributor being the US, followed by the UK, which provided the highest level of technology and equipment. Good cooperation between coalition members was highlighted, although Saddam Hussein had thought that Saudi Arabia would oppose the arrival of foreign forces on its soil, he was wrong, as the Saudi regime allowed US troops to be stationed in the country. At the same time, the international community cooperated to offer aid to Saudi Arabia, Turkey and Israel, all of which were considered possible victims of an Iraqi attack (Opriș 2001). Iraq also attempted to turn Israel against coalition forces by launching missiles over its territory, but this attempt was unsuccessful given the good cooperation and US-Israeli partnership (Collins 2019).

The shared political goals made cooperation, support between allied nations and coordination of the military operation possible so that it successfully achieved its goal (Beagle 2001, 54).

Conclusions

Joint operations are a collection of forces combined in either an alliance or coalition structure under a single command. Multinational participation has given these operations the necessary legitimacy within the system of international relations, while at the same time making action on the ground more effective because each

state contributes specialised forces, new techniques, and new methods to achieve the objectives set.

Operation Desert Storm is an example of such operations because the force structures of 36 states agreed on a common goal of the need to withdraw Iraqi troops from Kuwait, organised themselves under US command, contributed the necessary manpower and cooperated in the three environments. *Operation Desert Storm* also employed the latest technology of the time, which led to the operation's goal being achieved in a rapid timeframe, and the strikes had a high degree of precision with low collateral losses. *Operation Desert Storm* illustrates the benefits of incorporating new technologies into the military theatre as well as ground-to-air doctrine.

Over time, these operations have highlighted modern combat techniques that have advanced over generations to facilitate better field readiness. Future warfare as a military phenomenon will evolve with the evolution of post-modern society, but with the birth of the United Nations, multilateral disarmament and arms control have been central to the maintenance of international peace and security.

The transition period, reflecting past-present and present-future relations, will be characterized by numerous conflicts in which armies with doctrines, structures, and equipment specific to information societies will prevail. Asymmetric reactions to modern military action may be long-lived, taking the place of classic military conflicts, with disarmament as the evolutionary step and de-escalation becoming the high priority.

The qualitative, psycho-anthropo-sociological approach is based on a phenomenological, interpretative orientation. The data used are complex and rich in meaning and propose a new, modern perspective on the relationship between the signified (representation on the mental map) and the signifier (material representation).

The constructed analysis confirms the hypothesis that the security environment is shaped by the interplay between the paradigm of future war, speed, unpredictability, information innovation, and the desirable goal of disarmament, peace, and stability. Disarmament integrates a perspective that has been timely and recommended since ancient times, and war, though chameleonic, is essentially the same. Before being a politico-military phenomenon, it is a socio-psychological construct that engages destructive energies and mobilises hostilities in one form or another. When references are made to conventional weapons, terms such as *'arms limitation'* or *'arms control'* are used more often than *'disarmament'*. War, whatever its configuration, whatever its manifestations, is a dimension of a dispute, not a solution to it.

The post-modern era, as a result of the imbalances identified in the balance of power centres, as a result of technological gaps, strategic bottlenecks or limitations, brings to the fore the imminence of vulnerabilities and threats to security systems.

By dissecting the body of architecture of multinational operations assembled in an analytical manner of its own, including from the angle of the generational evolution of the history of warfare, this paper provides a broad perspective on the quality of systems interconnectedness in response to the challenges of today's global security environment. The most recent generation of warfare, the fifth, corroborates modern strategies in managing large-scale conflicts that are increasingly competitive across security horizontals and verticals.

References

Beagle, T. W. 2001. "Operation Desert Storm, Effects-Based Targeting. Another Empty Promise?" https://www.jstor.org/stable/resrep13830.12.

Collins, Shannon. 2019. "Desert Storm: A Look Back." https://www.defense.gov/News/Feature-Stories/story/Article/1728715/desert-storm-a-look-back/.

Enciclopedia Britannica. 2023. "Persian Gulf War." https://www.britannica.com/event/Persian-Gulf-War.

Englehardt, Lieutenant Colonel Joseph P. 1991. "Desert Shield and Desert Storm. A Chronology and Troop list for the 1990-1991 Persian Gulf Crisis." https://apps.dtic.mil/dtic/tr/fulltext/u2/a234743.pdf.

Frunzeti, Teodor. 2000. *Military Operations in Support of Peace.* Sibiu: Publishing House of the Land Forces Academy.

Georgescu, Gabriel. 2016. "Future Warfare as a Contemporary Military Phenomenon from the Perspective of Critical Infrastructure." *Bulletin of "Carol I" National Defence Univesity* 3 (3): 13-21.

Kaplan, Robert D. 2020. *The revenge of geography.* Bucharest: Litera Publishing.

Lind, William S., John F. Schmitt, și Gary I. Wilson. 1989. "The Changing Face of War: Into the Fourth Generation." *GLOBAL GUERRILLAS.* https://globalguerrillas.typepad.com/lind/the-changing-face-of-war-into-the-fourth-generation.html.

Ministry of National Defence. 2012. "Doctrine for Joint Operations." Bucharest: Tipografia Militară.

—. 2001. "The doctrine of the Romanian Army." Bucharest: Tipografia Militară.

Mocanu, Mircea. 2020. "Artificial Intelligence and beyond." *Defence and Security Monitor.* https://monitorulapararii.ro/inteligenta-artificiala-in-intelligence-si-nu-numai-1-28414.

Mureșan, Mircea. 2005. *Joint Operations in the War of the Future.* Bucharest: "Carol I" National Defence University Publishing House.

Mureșan, Mircea and Gheorghe Văduva. 2004. *The war of the future, the future of the war.* Bucharest: "Carol I" National Defence University Publishing House.

NATO. 2012. "NATO Glossary of Terms and Definitions." NATO Standardization Agency (NSA).

Opriș, Petre. 2001. "From «Desert Storm» to «Star Wars II»." *Military History Magazine* no. 2: 66.

Petrescu, Dan. 2021. "Military Art Course Support." Bucharest: Faculty of Security and Defence, "Carol I" National Defence University.

Toffler, Alvin. 1996. *Power in motion.* Bucharest: Antet Publishing.

U.S. Army Center of Military History. n.d.. "Operation DESERT STORM." Accessed January 29, 2023. https://history.army.mil/html/bookshelves/resmat/desert-storm/index.html.

UNSCR. 1990. "Resolution 678." *UNSCR - United Nations Security Council Resolutions.* http://unscr.com/en/resolutions/doc/678.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY
https://buletinul.unap.ro/index.php/en/

From mushrooms to artificial intelligence: technology's double-edges sword in enhancing soldiers

Maj. Sup. Inst. Gabriela NICOARĂ, Ph.D. Student*
Corporal Student Alex-Giulian COROI**

* "Carol I" National Defence University, Bucharest, Romania
e-mail: gabriela.nicoară.cj@gmail.com

** "Carol I" National Defence University, Bucharest, Romania
e-mail: scoroianu20@gmail.com

Abstract

This article entails a study of the methods for developing humans' capabilities to increase success rates during military conflicts. Hence, this scientific work encompasses a retrospective of the methods from antiquity by Sumerian, Viking, Greek, and Roman fighters, as well as a contemporary and prospective view of the methods of augmenting soldiers into "supersoldiers". Whether we refer to the first stage and initial attempts at developing soldier capabilities through mushrooms, alcohol, amphetamines, or to the revolutionary phase of this field through the involvement of technology, all these methods represent a „double-edged sword". This is because it involves, besides benefits, a series of ethical and legal concerns. Nevertheless, the article pledges the solution of augmenting soldiers and reinforcing troops, while simultaneously upholding ethical and legal norms.

Keywords:
human capabilities; artificial intelligence; supersoldiers; nanobots; ethical and legal concerns; approaches.

https://doi.org/10.53477/2284-9378-23-29

Global security represents an aspirational goal and nations strive to ensure a genuine defense potential in the event of armed conflict. Therefore, each state reinforces its troops and prepares its soldiers using various methods. Considering that the level of soldier preparation through natural approaches, such as adequate nutrition and fitness, it is no longer a desired benchmark and that real-world challenges demand a higher level of soldier capabilities, alternative methods are being considered. This scientific paper aims to analyze both the history of using war stimulants and the novel methods of augmenting the human essence employed among soldiers for troop consolidation. Given that all these methods raise a range of ethical and legal concerns that hinder their implementation, the article brings to attention a solution for transforming troops into a superior paradigm through the utilization of artificial intelligence.

A retrospective overview of enhancing soldiers' capabilities

Since the inception of humanity and the formation of tribes, military conflicts have been a constant presence in the world, serving as a means to obtain sovereignty over other regions. In recorded history, the first war took place around 2700 BCE between Sumer and Elam (Mark 2009), two ancient civilizations. Gradually, over time and through various battles, the value of well-trained warriors with developed physical and mental abilities was recognized. It was realized that these qualities actually dictate the success rate in combat. Thus, people identified various methods to extend common human limits.

The history of efforts to enhance soldiers' abilities dates back to ancient times when the Greeks and Romans consumed alcohol to numb their senses and boost their courage in battle (Bumbar 2015). This method was also employed in the Middle Ages, in the 16th century, when English soldiers were encouraged to drink beer before battles, and in the 17th century, when French soldiers were encouraged to use wine for the same reasons. During the period between the 8th and 11th centuries, infamous Scandinavian warriors known as "Vikings" were reputed for consuming both intoxicants and hallucinogenic mushrooms to augment their combat skills (Williams 2020). In this way, they gained a reputation in the eyes of other people and became known for their fury, aggression, strength, and bloody victories. Later, during the American Civil War (1861-1865), soldiers used morphine both for relaxation and pain relief (Jones 2020), and to prevent dysentery (Tackett 2022).

Over time, stimulants have undergone a shift in perception. Lukasz Kamienski, a professor of political science at the Institute of American and Polish Diaspora Studies and author of the book "Shooting Up: A Short History of Drugs and War," observed an interesting phenomenon: cocaine had also been used as a substance of abuse on the frontline during wars. It was used to amplify energy, combat fatigue, and reduce anxiety. The drug gained widespread popularity when the British army developed a

combination of cocaine and caffeine called "Forced March" (Bourke 2010), which was then self-prescribed by individuals as a means to cope with the challenges of conflict.

During World War II, the Nazi regime utilized Pervitin, a pill form of amphetamine patented in 1937, to enhance soldiers' performance in combat (Pruitt 2019). Pervitin was administered to soldiers to boost their self-confidence, increase physical energy, and combat fatigue, a technique to create perfect soldiers for the infamous Blitzkrieg (Andreas 2020).

On the other hand, during World War II, the Nazi regime not only administered drugs to its soldiers but also conducted a series of experiments with the aim of creating a superior race of soldiers. These experiments were carried out by the scientific division of the Nazi regime, Ahnenerbe, and aimed at enhancing soldiers through various means, including genetic engineering and other techniques (Charney 2015). One of the main objectives of these experiments was to create stronger, faster, and more resilient soldiers. Ahnenerbe conducted a series of experiments in an attempt to achieve this goal, including procedures on human subjects involving injection with various substances and exposure to extreme conditions. Despite Ahnenerbe's efforts, these experiments ultimately proved to be unsuccessful. Many of the subjects of these experiments suffered severe injuries or died as a result of the procedures, and the Nazi regime failed to create a superior race of soldiers. Consequently, the experiments were abandoned.

Attempts to create "supersoldiers" are not limited to these examples, as history is replete with such endeavors, exploring a wide range of alcohol-based products, plants, mushrooms, and medicinal substances. Just like the Nazi regime, while the "Ahnenerbe" program ventured into bolder territory, many other organizations, such as the Defense Advanced Research Projects Agency (DARPA), have leveraged technological advancements to shift the direction of creating "supersoldiers" (Shah 2019, 10).

A contemporary and prospective overview of creating supersoldiers

The concept of supersoldier has been a constant presence in science fiction literature and superhero narratives for decades, and it has also been explored in certain military and scientific circles as a potential future direction for military technology. Essentially, a supersoldier is a hypothetical type of soldier who has been genetically or technologically enhanced to possess supernatural physical and mental abilities. This concept is complex and multifaceted, touching upon a wide range of issues related to military technology, human enhancement, and the boundaries of what is possible for humanity.

https://doi.org/10.53477/2284-9378-23-29

As technology and other fields have advanced, the subject of creating supersoldiers has become increasingly debated. Thus, the field of "Human Performance Enhancement" (HPE) has emerged, which has seen significant development in the United States, China, and Russia, as well as some European and Asian countries such as the United Kingdom, France, Japan, South Korea, etc. (Blumenthal, Hottes and Foran 2021, 4) Its main objective is to develop the physical and mental capabilities of soldiers, endowing them with supernatural abilities. As a result, numerous methods have been identified, with the most relevant ones including genetic engineering, cybernetic implants, exoskeletons, nanotechnology, wearable devices, performance-enhancing substances, and artificial intelligence.

Studied by the United States Department of Agriculture (USDA), the National Institutes of Health (NIH), the Food and Drug Administration (FDA), and the European Molecular Biology Laboratory (EMBL), genetic engineering is a technology that allows scientists to manipulate or modify the genetic material of an organism to alter or enhance certain characteristics. In the military context, this could involve modifying the genes of military personnel to provide them with improved physical or cognitive abilities. For example, they could receive genes that make them stronger, faster, more intelligent, and more resilient to diseases, or, according to the Nuffield Council on Bioethics, enhance their night vision and develop a sense of smell (Shah 2019, 7). Additionally, genetic engineering is recognized as a significant method for eradicating malaria (Callaway 2015).

Cybernetic implants are being addressed by Neuralink, a company founded by Elon Musk, focusing on brain-machine interfaces and other neural implants; Paradromics, a company developing high-bandwidth neural implants for medical and military applications; and DARPA, the research organization of the US Department of Defense. These implants represent surgically implanted devices designed to enhance specific abilities. They may encompass implants that augment strength, speed, or resilience or provide sensory enhancements, such as highly developed vision or hearing. In addition to enhancing these senses, cybernetic implants serve as the foundation for restoring these abilities in soldiers who have lost them during combat by introducing digital auditory or visual information into the brain (Brownie 2016).

Exoskeletons are significantly developed, particularly in the United States (by organizations such as DARPA and the Tear Research Program for Tele-Empowerment and Augmentation), as well as in Japan and South Korea. Exoskeletons are wearable devices designed to enhance the strength and endurance of the user (Keller 2022). They are worn over the user's clothing and powered by hydraulic motors or other mechanical systems. In military contexts, exoskeletons can aid soldiers in transporting heavy loads over long distances or provide additional protection in combat situations. Some exoskeletons are designed to be lightweight and agile, enabling rapid and effortless movement, while others are heavier and

designed for tasks requiring substantial power, such as lifting heavy objects or carrying large backpacks. Exoskeletons have the potential to revolutionize the performance of soldiers and represent an active area of research and development.

The manipulation of matter at the atomic and molecular scale, known as nanotechnology, is a field pursued by the three global superpowers and holds significant potential for military applications. In this context, technology can empower soldiers with enhanced abilities, such as improved senses and intelligence, as well as enhanced medical conditions. With dimensions smaller than 500 nm. (Soto, et al. 2020, 14), nanobots can be employed to administer medication with high efficiency. Typically, medications act systemically before reaching the affected area. With the aid of nanotechnology, medication can be precisely targeted, significantly enhancing effectiveness and reducing the likelihood of side effects, enabling soldiers to be healed before symptoms even manifest.

Wearable devices are another key technology for enhancing soldiers. They can take various forms, including smartwatches, head-mounted displays, and clothing embedded with sensors. Wearable devices can provide soldiers with real-time situational awareness, allowing them to know the whereabouts of their teammates, local weather conditions, and even their vital signs. This information can be extremely valuable in combat situations as it enables soldiers to make better-informed decisions and respond more quickly to changing circumstances.

Performance-enhancing substances (PEDs) offer a valuable advantage in situations where soldiers are required to perform at the highest level. These substances are used to enhance both the mental and physical capabilities of soldiers. Firstly, stimulant medications such as amphetamines can increase alertness and reduce fatigue, which is beneficial for soldiers who need to maintain a high level of vigilance over long periods. Similarly, other substances like modafinil have been shown to improve cognitive performance and vigilance, which can be useful for soldiers who need to make rapid and precise decisions in stressful situations. Secondly, these stimulants refer to anabolic steroids, which can increase physical strength by 5 to 20 percent. These medications are often used by athletes in sports that require sudden bursts of energy, such as powerlifting and football. However, most sports prohibit PEDs, and their use can lead to negative side effects such as cardiovascular and hepatic injuries, increased aggression, and alterations in sexual characteristics (Scharre and Fish 2018).

Due to the multifaceted nature of roles within a military system, there is no "one-size-fits-all" solution for enhancing soldiers' capabilities, as they are positioned in diverse situations and assigned a wide range of missions. The methods used to enhance soldiers' performance depend on their specific tasks, and a multitude of enhancement techniques are employed to optimize their effectiveness. Whether it is wearable technology, exoskeletons, chip implants, or nanotechnology, these will be implemented through artificial intelligence, which, in our opinion, will innovate multiple industries.

https://doi.org/10.53477/2284-9378-23-29

Artificial intelligence (AI) is increasingly recognized and utilized in today's world and is developing at a rapid pace. In the military domain, countries such as the United States (DARPA), China, and Russia are exploring this field to enhance human capabilities. AI has the potential to revolutionize the way soldiers are trained and deployed on the battlefield. By leveraging AI technology, military forces can significantly enhance their capabilities and efficiency in various missions. One way AI can be used to enhance soldiers is through the development of intelligent assistants and wearable devices that can assist soldiers in various tasks. These devices can provide soldiers with real-time information about their surroundings, alert them to potential threats, and aid them in navigation and communication. For example, a soldier wearing an AI-equipped smart helmet could receive alerts about approaching enemy fire or be guided through a hazardous area. AI can also be used to improve soldiers' training. By simulating different scenarios and environments, AI can provide soldiers with realistic training experiences that better prepare them for the demands of the battlefield. This can contribute to reducing the risk of human casualties and improving the overall effectiveness of military forces (Blumenthal, Hottes and Foran 2021, 4).

Being a relatively new and highly interesting field, numerous companies worldwide are rapidly engaging in AI research. On November 30, 2022, "OpenAI," a company founded by a consortium in collaboration with Elon Musk, released a free AI program called "Chat GPT" to the public, showcasing the remarkable benefits of AI. It is an AI-powered assistant designed to help and provide useful information in multiple languages across a wide range of topics. Trained using massive amounts of textual data, Chat GPT processes and generates text almost instantaneously in various contexts, making it an incredibly useful tool for a wide range of applications. For instance, it is capable of understanding and can be applied in various conversational applications such as building chatbots, virtual assistants, creating interactive conversation interfaces for games, websites, solving integrals, and even debugging lines of code. Chat GPT3 (the current version) runs on a neural model of 175 billion characters, and Elon Musk's promise is to develop ChatGPT4 in 2023, which runs on 100 trillion characters. Essentially, in one year, it will become 571 times more powerful, faster, and more efficient.
Therefore, considering the capabilities of an AI-based program and observing how easily it can be employed, in the near future, AI will become a powerful tool and innovate numerous industries, especially military services.

Ethical and legal concerns regarding the creation of supersoldiers and troop enhancement

Although we have powerful tools for developing supersoldiers and intelligent systems for enhancing military troops, certain factors still prevent us from taking the army to a higher level. Thus, we are constrained by ethical and legal concerns. In

general, the ethical and legal issues surrounding soldier enhancement are complex and multifaceted. Special attention must be paid to the potential risks and benefits of any proposed enhancements, and measures must be taken to ensure that they are used ethically, legally, and responsibly. There are several ethical and legal issues that arise when considering soldier augmentation. These issues can be broadly grouped into four categories: ethical aspects related to the welfare of soldiers, the welfare of the military society as a whole, the potential for abuse or misuse of technologies, and legal aspects.

The primary ethical concern related to soldier enhancement is the risk of compromising their physical and mental integrity. Some enhancements, such as performance-enhancing drugs, may have negative side effects or long-term consequences for health. For example, there is potential for enhancements to cause psychological harm, such as altering a soldier's sense of self or creating feelings of dependency. There is also the possibility of the technology implemented in soldiers' bodies becoming faulty, leading to irreversible consequences.

The implementation of artificial intelligence systems results in job obsolescence. As technologies become more advanced and precise, they may be capable of performing tasks that were previously carried out by human employees. This could lead to military personnel being displaced and disruption within the entire military industry. There is a risk of enhancements being corrupted or compromised through cyberattacks and used to control or manipulate soldiers, or to be used for nefarious purposes, such as creating killing machines. Additionally, enhancements can lead to errors that result in serious consequences.

In addition to ethical concerns, there are also jurisdictional concerns. This is due to the lack of specialized legislation addressing the ramifications of these new technologies. For example, in the event that an autonomous weapon system incorrectly identifies a group of non-combatants as hostile enemies and initiates attacks (as programmed), there will be no recourse for the resulting victims.
Considering the availability of such powerful tools for creating "supersoldiers" and the potential for fortifying troops with artificial intelligence systems, ethical and jurisdictional issues hinder or at least slow down these endeavors.

Approaching the creation of supersoldiers compliance with ethical and legal concerns

In an ethically guided society, maintaining the physical and mental health of soldiers and protecting human integrity is a parameter of normality. Therefore, procedures for soldier enhancement that involve risks to their physical and mental well-being need to be reassessed. Solutions can be identified to mitigate the negative impact created by the implementation of these technologies on individuals' livelihoods.

https://doi.org/10.53477/2284-9378-23-29

Human oversight during the initial implementation phase of innovations is one such solution. As systems become so advanced and precise that human presence is no longer necessary, human personnel will be notified in advance, and appropriate solutions will be found to address unemployment. For example, redistributing employees to areas where there is a staff shortage, reducing the workload of a position to make it shareable with another employee, thereby increasing efficiency, or simply transferring them to reserves and ensuring pensions. Thus, in the end, society can significantly benefit from the implementation of these technologies, even though it may initially pose a complex challenge with negative repercussions for employees.

New technologies come with risks, but compared to those associated with human activity, they are much smaller. We consider that, like humans, the new technologies will also be vulnerable to corruption through cyberattacks and system overload, compared to corruption at the leadership level or fatigue experienced by humans. However, certain human characteristics that lead to frequent errors will no longer be present, such as negligence, lack of interest, personal issues, and other situations faced by personnel. It is expected that at the beginning of implementing these new technologies, errors will be identified, but they can be improved until the incident rate approaches zero.

Legal issues are inherent in the implementation of such systems. If the technology makes errors, no individual can be held accountable under current regulations. However, this lack of liability is not a negative factor. It is important to recognize that holding someone responsible for an error does not guarantee that the problem will be resolved or that errors will not recur. Inevitably, issues and errors will always exist, and it is unconstructive to seek blame and impose sanctions, other than addressing and fixing the error itself. Otherwise, it would be only a superficial form of redressing the harm. Therefore, it is necessary to stop the respective system, followed by identifying solutions that contribute to software improvement. Additionally, after the implementation and deployment of the system, developers will carefully analyze its functionality and provide updates.

Conclusion

The augmentation of military personnel is a delicate matter governed by ethical and legal norms that prohibit the creation of "supersoldiers." This is because the procedures used for military augmentation carry inherent risks and may compromise the integrity of individuals. Therefore, the methods previously mentioned can be considered a "double-edged sword" as they offer both benefits and ethical and legal challenges.

Even though „supersoldiers" created using the aforementioned methods may bring significant advantages in military conflicts, and their utilization may not have

immediate negative effects, soldiers can suffer long-term consequences. Therefore, considering the rapid advancement of technology (as is the case with ChatGPT), we believe that the legal implementation of such systems will occur in the near future, once these technologies reach a highly developed level that ensures the protection of soldiers' integrity to a near 100% extent.

However, in the present context, a solution could be considered fortifying troops with AI-based systems. This way, we can avoid compromising soldiers' integrity and altering their natural structure through genetic engineering, chip implantation, nanobots, and so on. Instead, by utilizing AI-based devices, we can achieve a consistent set of advantages within the Romanian armed forces. Some of these advantages include the efficient optimization of the military structures' logistics system, adapting medical structures to the requirements of current armed conflicts, supporting decision-making in the operational planning process, and addressing personnel shortages. Thus, integrating Artificial Intelligence systems within the military can bring significant benefits both at an individual level and for the military society as a whole.

At an individual level, young logisticians can save time and resources by utilizing an AI-integrated logistics system. These systems can be programmed to understand document structure and content, allowing them to automatically generate the appropriate documents based on the situation. They can also be programmed to fill out forms and identify and correct errors in documents, including invoices, contracts, repair orders, or any other document necessary in the logistics process.

Integrating an AI-based medical system within the military can provide significant benefits to soldiers. These benefits include more accurate diagnoses and more effective treatments tailored to the needs of each individual. By utilizing machine learning algorithms and understanding data from previous experiences, the system can provide a diagnosis closer to reality and suggest more efficient treatments. It can also be used to monitor the individual health of soldiers and prevent illnesses. These benefits can help improve soldiers' conditions for successful mission completion.

Implementing AI-based security and defense systems can bring numerous advantages to the military personnel involved in security and combat operations. These benefits include enhanced security, surveillance, and recognition through the use of image recognition algorithms, enabling quicker and more precise identification of suspicious objects or individuals, intrusion detection in secure areas, and efficient monitoring of terrains. Additionally, integrating sensor-guided technology with AI can improve the accuracy and effectiveness of artillery, thus minimizing collateral damage and providing better protection for soldiers and civilians involved in military operations.

At the societal level of the military as a whole, systems based on such technology can significantly reduce human labor, resource consumption, and time. AI systems can

be programmed to identify issues in the supply chain and make quick and precise decisions to ensure a continuous flow of resources to the operational zone, optimizing the entire logistics space. Furthermore, once these technologies are implemented and reach an advanced stage of development, human presence becomes redundant in the regions where these systems are deployed. As a result, human personnel can be redistributed to areas with a shortage of workforce, addressing the personnel gaps present in military units. Implementing these systems will solve the existential problems of the armed forces and significantly reduce human errors since these systems will be programmed to perform specific functions with precision and rigor. In the event of errors, the solution is much simpler, involving software updates, as opposed to lengthy and complex legal processes against individuals.

References

Andreas, Peter. 2020. "How Methamphetamine Became a Key Part of Nazi Military Strategy." *Time Magazine.* https://time.com/5752114/nazi-military-drugs/.

Blumenthal, Marjory S., Alison K. Hottes și Christ Foran. 2021. "Technological Approaches to Human Performance Enhancement." https://www.rand.org/pubs/research_reports/RRA1482-2.html.

Bourke, Joanna. 2010. "Enjoying the high life-drugs in history and culture." doi:https://doi.org/10.1016/S0140-6736(10)62153-8.

Brownie, Ryan. 2016. "U.S. military spending millions to make cyborgs a reality." *CNNpolitics.* https://edition.cnn.com/2016/03/07/politics/pentagon-developing-brain-implants-cyborgs/index.html.

Bumbar, Micky. 2015. "How Alcohol Played a Key Role in Warfare around the World." https://lordsofthedrinks.org/2015/05/09/how-alcohol-played-a-key-role-in-warfare-around-the-world/.

Callaway, Ewen. 2015. "Mosquitoes engineered to pass down genes that would wipe out their species." doi:https://doi.org/10.1038/nature.2015.18974.

Charney, Noah. 2015. "Did Nazis really try to make zombies? The real history behind one of our weirdest WWII obsessions." https://www.salon.com/2015/08/22/did_nazis_really_try_to_make_zombies_the_real_history_behind_one_of_our_weirdest_wwii_obsessions/.

Jones, Jonathan S. 2020. "The Great Risk of Opium Eating: How Civil War-Era Doctors Reacted to Prescription Opioid Addiction." https://library.medicine.yale.edu/blog/great-risk-opium-eating-how-civil-war-era-doctors-reacted-prescription-opioid-addiction.

Keller, John. 2022. "Army asks industry about the latest in exoskeletons to improve soldier performance and physical endurance." https://www.militaryaerospace.com/unmanned/article/14270047/exoskeletons-soldier-performance-physical-endurance.

Mark, Joshua J. 2009. "War In Ancient Times." https://www.worldhistory.org/war/.

Pruitt, Sarah. 2019. "Inside the Drug Use That Fueled Nazy Germany." https://www.history.com/news/inside-the-drug-use-that-fueled-nazi-germany.

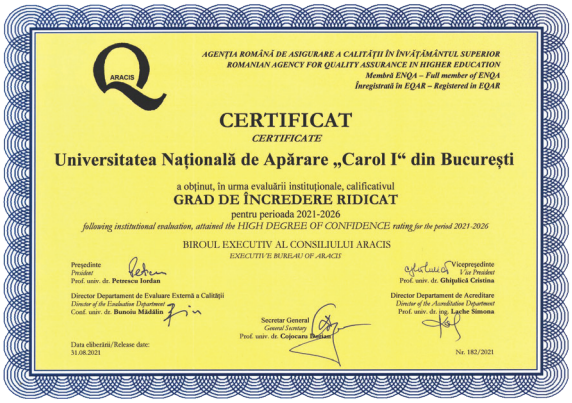
Scharre, Paul și Lauren Fish. 2018. "Human Performance Enhancement." https://www.jstor.org/stable/resrep20411.

Shah, Morial. 2019. "Genetic Warfare: Super Humans And The Law." *North Carolina Central University Science and Intellectual Property Law Review* 12 (1): 24. https://archives.law.nccu.edu/cgi/viewcontent.cgi?article=1044&context=siplr.

Soto, Fernando, Jie Wang, Raijb Ahmed și Utkan Demirci. 2020. "Medical Micro/Nanorobots in Precision Medicine." https://doi.org/10.1002/advs.202002203.

Tackett, Brittany. 2022. "Drug Use in Wartime." Edited by Kelly Doran. *American Addiction Centers.* https://recovery.org/addiction/wartime/.

Williams, Keith. 2020. "Drugs Used in Conflict and Wars, Part 1: Vikings' Early Use of a Performance-Enhancing Drug?" https://www.caymanchem.com/news/drugs-used-in-conflict-and-wars.



AGENȚIA ROMÂNĂ DE ASIGURARE A CALITĂȚII ÎN ÎNVĂȚĂMÂNTUL SUPERIOR
ROMANIAN AGENCY FOR QUALITY ASSURANCE IN HIGHER EDUCATION
Membră ENQA – Full member of ENQA
Înregistrată în EQAR – Registered in EQAR

CERTIFICAT
CERTIFICATE

Universitatea Națională de Apărare „Carol I" din București

a obținut, în urma evaluării instituționale, calificativul
GRAD DE ÎNCREDERE RIDICAT
pentru perioada 2021-2026
following institutional evaluation, attained the HIGH DEGREE OF CONFIDENCE rating for the period 2021-2026

BIROUL EXECUTIV AL CONSILIULUI ARACIS
EXECUTIVE BUREAU OF ARACIS

Președinte
Președinte
Prof. univ. dr. Petrescu Iordan

Vicepreședinte
Vice Președinte
Prof. univ. dr. Ghițulică Cristina

Director Departament de Evaluare Externă a Calității
Director of the Evaluation Department
Conf. univ. dr. Bunoiu Mădălin

Director Departament de Acreditare
Director of the Accreditation Department
Prof. univ. dr. ing. Lache Simona

Secretar General
General Secretary
Prof. univ. dr. Cojocaru Bogdan

Data eliberării/Release date:
31.08.2021

Nr. 182/2021

EDITOR
„Carol I" National Defence University Publishing House
(Highly appreciated publishing house within "Military science, intelligence and public order" of Titles, Diploma and University Certificates Awards National Council)
Adress: Panduri Street, no. 68-72, Bucharest, 5th District
e-mail: buletinul@unap.ro
Phone: +4021.319.48.80 / 0365; 0453

Signature for the press: 07.07.2023
The publication consists of 194 pages.

480/07.07.2023

C.112/2023