ROMANIAN MILITARY THINKING

ERIH PLUS
EUROPEAN REFERENCE INDEX FOR THE HUMANITIES AND SOCIAL SCIENCES
INDEX COPERNICUS INTERNATIONAL
DOAJ
Central and Eastern European Online Library
MIAR
Matriz de Información para el Análisis de Revistas
EBSCO
ROAD
DIRECTORY OF OPEN ACCESS SCHOLARLY RESOURCES

FOUNDED IN 1864 UNDER THE NAME "ROMÂNIA MILITARĂ"
- NEW SERIES, YEAR XX -

3/2024

JOURNAL OF MILITARY SCIENCE AND SECURITY STUDIES PUBLISHED BY THE DEFENCE STAFF

PUBLISHER
THE DEFENCE STAFF

EDITORIAL OFFICE
București, str. Izvor nr. 110, sector 5
Postal code: 050564
Telefon: +4021.319.48.80/1005597; 1005596
Tel./fax: +4031.426.09.90
E-mail: gmr@mapn.ro
Web: gmr.mapn.ro

Printed
at Military Technical Publishing Centre
C ___/2024 B 766/10.09.2024

ROMANIAN MILITARY THINKING

Journal of Military Science and Security Studies Published by the Defence Staff

Founded in 1864 under the name *"România Militară"*
– new series, year XX –

ISSN Print: 1841-4451
ISSN Online: 1842-824X
10.55535/RMT.2024.3

Romanian Military Thinking is a scientific journal with acknowledged prestige in the field of "*Military Science, Intelligence and Public Order"*, in keeping with the evaluation carried out by the National Council for Titles, Diplomas and Certificates (CNATDCU) in 2011 (http://www.cnatdcu.ro/wp-content/uploads/2011/11/reviste-militare1.pdf)

Romanian Military Thinking Journal is included in the Journal Master List of the **ERIH PLUS, INDEX COPERNICUS INTERNATIONAL, DOAJ, CEEOL, MIAR, EBSCO's** and **ROAD Catalogue**

A LEGACY SINCE 1864

The Romanian Armed Forces road to modernity started in 1859, once the United Principalities General Staff Corps, currently the Defence Staff, was established.

Soon after it, in 1864, a group of nine captains, graduates of the first series of the Officer Cadet School in Bucharest, took the initiative to develop a *"military science, art and history journal"* named *"România Militară/Military Romania"*.

The initiators of the publication – **G. Slăniceanu** (Captain, Chief of the Engineer Battalion), **A. Gramont** (Staff Captain), **G. Borănescu** (Engineer Captain), **G. Anghelescu** (Staff Captain), **A. Anghelescu** (Artillery Captain), **E. Arion** (Artillery Captain), **E. Boteanu** (Staff Captain), **E. Pencovici** (Staff Captain) and **C. Barozzi** (Engineer Captain) –, educated not only in Romania but also abroad, were inspired by the necessity to develop a substantial theoretical activity in the Romanian Army too.

The journal manifesto[1], included in the first issue, which appeared on 15 February 1864, contained innovative ideas and approaches that were meant to:

"- contribute to the organisation of our military system the Legislative Chamber is about to decide upon soon;

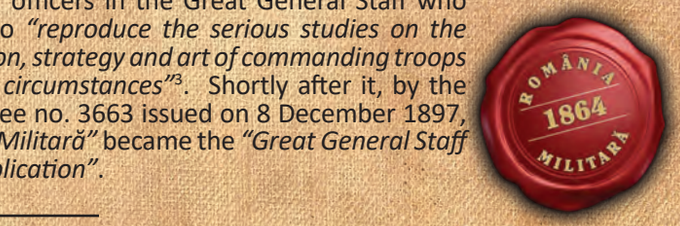
- assemble and examine the Country old military institutions that had made for the glory of Romania for several centuries and ensured our existence;

- explore, in the absence of any military study, all the aspects related to the Army training, the most solid basis of the armed forces;

- get the Romanian Troops well-informed about the military events in the world;

- join efforts to work concertedly and whole-heartedly to develop and strengthen the edifice that is meant to ensure the future of our country"[2].

"România Militară" was an independent publication, under the aegis of the War Ministry, and it ceased to appear in 1866 as there were no sufficient funds and subscribers. The publication was resumed in 1891, about a quarter of a century later, also as the result of the initiative of a group of officers in the Great General Staff who intended to *"reproduce the serious studies on the organisation, strategy and art of commanding troops under any circumstances"*[3]. Shortly after it, by the Royal Decree no. 3663 issued on 8 December 1897, *"România Militară"* became the *"Great General Staff official publication"*.



[1] *Din trecutul României Militare cu prilejul aniversării a 75 de ani de la apariția ei în viața armatei. 1864-1939*, București, 1939, p. 31.

[2] *Ibidem*, p. 32.

[3] *România Militară*, no. 1, 1981, p. 6.

English version by **Diana Cristiana LUPU**.

C. Barozzi
(Engineer Captain)

E. Pencovici
(Staff Captain)

E. Boteanu
(Staff Captain)

G. Borănescu
(Engineer Captain)

G. Anghelescu
(Staff Captain)

A. Gramont
(Staff Captain)

E. Arion
(Artillery Captain)

G. Slăniceanu
(Captain, Chief of the Engineer Battalion)

A. Anghelescu
(Artillery Captain)

The *GÂNDIREA MILITARĂ ROMÂNEASCĂ*
Journal Awards
are yearly bestowed,
by the Romanian Armed Forces Defence Staff,
on the most valuable works in the field
of military science, published in the previous year

"Brigadier General Constantin Hîrjeu" Award

"Lieutenant Colonel Mircea Tomescu" Award

"Division General Ştefan Fălcoianu" Award

"Army Corps General Ioan Sichitiu" Award

"Marshal Alexandru Averescu" Award

CONTENTS

DISRUPTIVE AND EMERGING TECHNOLOGIES IMPACT ON THE MULTINATIONAL JOINT OPERATIONS COORDINATION IN MODERN WARFARE

Major General Valerică VRĂJESCU
Commander of "General Ioan-Emanoil Florescu" Joint Forces Command

New technologies are rapidly emerging in various fields and many technological advances are considered innovative, but not each and every technology will change the ways of waging wars. However, there are technologies that have an exponential and sometimes decisive impact on modern warfare in terms of introducing new paradigms, creating new combat domains, adapting or changing operational doctrines and concepts etc. Therefore, it is important to understand the use of current disruptive and emerging technologies and their impact on modern warfare.

Military operations have long posed challenges to national security practitioners. In modern warfare, the emphasis is on joint and multi-domain military operations, which represent an evolution in military strategies, as the mentioned concepts entail integrating and coordinating forces in all areas of operations (air, land, maritime, cyberspace and space). These types of operations meet the requirements of a complex and multidimensional combat environment, where success depends on the ability to effectively integrate various capabilities and manoeuvre them in different domains simultaneously. Modern history demonstrates that military operations are conducted not only by states in declared conflict or competition, but also by "proxy" states or military organizations financed by them. Alliances are thus punctually formed in order to meet national interests.

In this context, the development of disruptive and emerging weapon systems has the potential to increase the complexity of the organization and conduct of military operations. An example in this regard is that of NATO, which faced significant challenges during the air operations in Kosovo in 1999 because the encrypted radio systems used by some member states could not communicate with those of other states. Lately, allies have had substantial debate over the best policies and practices to guide cyber operations. Nowadays, the weapon systems based on disruptive technologies will present new challenges

in relation to interoperability and, above all, the decision-making process. Certainly, these challenges will not be insurmountable… just as allies have integrated advanced technologies such as GPS and nuclear weapons into planning and conducting operations, they will also succeed in integrating the new disruptive and emerging technologies into these processes. This aspect will profoundly change the conduct of joint, especially multinational, operations, influencing the manner in which they are planned, coordinated and executed, while information warfare will play a major role in maintaining (or disrupting) such operations. The mentioned changes will occur at all levels, including forces integration, increased interoperability, accelerated decision-making and increased operational efficiency.

Multinational Joint Operations and Disruptive Technologies Conceptualization

Alliances and coalitions are cooperative efforts to which their members contribute resources to pursue common security interests. Alliances are typically more deeply formalized institutions whose operations are codified in treaties, while coalitions are shorter-term arrangements made to accomplish specific tasks – such as defeating a conjunctural adversary. In the current security environment, states often conduct military operations alongside allies or coalition partners. These multinational efforts generate both political and operational benefits. Politically, multinational operations can provide the use of force with greater legitimacy than unilateral actions, and the involvement of multiple states helps signal that a military operation is justified. Alliances and coalitions also allow for sharing tasks, each member state contributing to the planning and conduct of military operations. It can reduce pressure on any ally's military in the event of short-term action, allowing states to leverage the specialized capabilities of the armed forces of different alliance or coalition members.

Despite their virtues, alliance and coalition operations also pose obstacles to strategic and operational coordination. Even if allies share common security interests, they may have trouble with agreeing how to pursue their goals – a task that becomes increasingly difficult as the number of states in an alliance or coalition grows and if the terms of the alliance engagement are vague (as they are often formulated to prevent them from being drawn into conflicts they would prefer to avoid). At the operational level, allies and partners may face challenges when working together because of the differences in terms of technical, cultural or procedural factors. Disruptive technologies have the potential to exacerbate all the mentioned differences.

The term disruptive technology refers to a new type of technology that invariably makes existing technology obsolete. It is an innovative technology that triggers sudden and unexpected effects. In the military field, a disruptive technology will provide its possessor with a decisive and exponential advantage. Moreover, its use could result in a definitive victory and its impact would lead to a paradigm shift in the nature and conduct of military operations, rendering one or more core competencies of war obsolete or irrelevant.

Robotics, satellites, drones, cyber warfare, nanotechnology, Artificial Intelligence, the Internet of Things (IoT), stealth technology, blockchain and data security, augmented and virtual reality, biotechnology and human augmentation are examples of militarily usable disruptive and emerging technologies. States around the world have already launched military systems that are based on such technologies. Military decision-makers view these systems as ways to increase the efficiency and reduce the risk of military operations. Process automation such as signal processing can reduce manpower requirements, while replacing front-line military with remotely operated weapon systems, which can mitigate the political risks associated with casualty suffering.

As states develop disruptive and emerging technologies, leaders must consider the challenges that may arise when deploying these technologies as part of larger alliance or coalition efforts. Firstly, alliance leaders should consider the uneven rates at which alliance members will be able to adopt these new technologies and the consequences that this aspect could have on alliance and coalition operations. Secondly, leaders should consider how disruptive technologies can affect two important components of alliance dynamics: interoperability and shared decision-making.

Advantages of Adopting Disruptive and Emerging Technologies in Multinational Joint Operations

The new technologies development pace is not the same worldwide, which means that some states will possess and effectively operate capabilities based on modern technologies, while others will not have access to such capabilities to the same extent. This uneven distribution of technology may result from variation in material and human resources or political resistance to adoption. Allies with developing economies will tend to allocate funding to modernizing conventional equipment rather than to developing new military capabilities based on emerging and disruptive technologies. In addition to variation in material resources, public support for the development of emerging military capabilities varies significantly from state to state, which may also influence the way states develop such technologies. Even though autonomous weapon systems enable the execution of a wide range of military missions, the notion of weapons – robots or weapons controlled by artificial intelligence – often creates negative images in public perception. Moreover, states without emerging technology-based capabilities may be less able to contribute to missions, which may compel better-equipped allies to assume a greater share of the effort, which can create friction.

The integration of disruptive technologies would stimulate military commanders to think and use them at the operational and tactical levels of war, and political leadership would likely exercise options at the strategic level. However, the disruptive potential of these technologies requires understanding how they could fundamentally affect the nature of military operations. Here are some specific ways in which emerging and disruptive technologies will impact the leadership and execution of these types of operations:

1. Interoperability and advanced integration

- ***Joint digital platforms:*** *The development of integrated command and control platforms, based on artificial intelligence and big data, will enable the joint and partner nations to rapidly and efficiently share information. It will ensure*

a common understanding of the situation and more effective coordination.

- ***Combat engagement:*** *Emerging technologies such as robotics, satellites, drones etc., becoming mature, are causing the rules of engagement in war to change; for example, stand-off operations/non-contact warfare may become the norm in the future, drastically reducing the risk to the troops. UAVs define new rules of engagement, and concepts like drone swarm tactics will provide a new method for engaging the adversary. New domains of warfare will open up, such as space, cyberspace, virtual domain, including social media.*
- ***Secure communication:*** *Advanced communications technologies such as 5G and encrypted networks will significantly improve the ability of multinational forces to communicate seamlessly and without the risk of compromising data security, even in environments that are hostile or have limited infrastructure.*

2. Rapid decision and real-time information

- ***Artificial Intelligence and data analysis:*** *Artificial Intelligence (AI) will enable the rapid collection and processing of large volumes of data from various sources (drones, satellites, ground sensors), and commanders will be able to make informed decisions in real time, reducing the period needed to respond and adapt to changes in the battlefield.*
- ***Autonomous systems:*** *The use of drones and other autonomous systems will provide a constant flow of tactical information, and AI will be able to suggest strategic actions based on this information, thereby optimizing decision-making at all levels.*

3. Efficient coordination and synchronization

- ***Virtual simulations and training:*** *Virtual and augmented reality, along with advanced simulations, will allow multinational forces to train together in a joint virtual environment, even if they are in different locations. These simulations will be more realistic and allow tactics to be tested in a hostile environment.*

- ***Automated planning:*** *Emerging technologies will automate planning processes, creating multiple scenarios based on available data, optimizing available resources for better coordination among multinational forces.*
- ***Movement:*** *AI tools can improve mobility by automatically suggesting ideal routes, taking into account traffic congestion, road conditions, broken bridges and other elements. Intelligent ground, air and underwater vehicles can improve the range of surveillance and weapon systems.*

4. Multinational capabilities improvement

- ***Logistics and supply:*** *Logistics management systems based on blockchain and AI will provide transparency and efficiency in managing shared resources. Multinational forces will be able to better coordinate the supply and use of resources, avoiding duplication of effort and reducing waste.*
- ***Distributed manufacturing technologies:*** *3D printing and other additive manufacturing technologies will enable the on-site production of the necessary equipment, reducing reliance on traditional supply chains and better adapting to the specific needs of each participating force.*
- ***Protection:*** *Equipment and personnel protection will certainly get a boost. Nanofiber-based military uniforms could change colour and texture to better camouflage, thus reducing the visual signature, and inventions like smart robots, drones, UCAVs etc. will reduce the involvement of troops/pilots in risky situations and therefore casualties on the battlefield.*

5. Decision and risk management

- ***Collaborative decision-making platforms:*** *Digital platforms that enable communication between the armed forces of the Alliance or coalition states will make it easier to manage multinational joint operations, facilitating the exchange of sensitive information and the synchronization between different levels of command.*
- ***Risk and conflict management:*** *AI and predictive analytics will help anticipate and manage potential conflicts between*

participating nations, be they related to differences in doctrine, communication or strategic interests.

6. Cyber and information operations

- ***Joint cyber defence:*** *Emerging technologies will enable the development of joint cyber defence frameworks so that multinational forces can concertedly defend their critical infrastructure and communications against cyber attacks.*
- ***Information operations:*** *Multinational collaboration in information operations will be enhanced by emerging technologies, which will enable better coordination in the fight against disinformation and propaganda, especially in areas of complex operations and those of strategic interest.*

7. Security and modern warfare ethics

- ***Ethical considerations:*** *As emerging technologies become more integrated into military operations, ethical challenges will arise related to the use of AI in lethal decisions, the compliance with international laws, and the protection of human life. Multinational forces will need to develop common legislation to govern the use of these technologies.*

Challenges related to Decision Making in Ensuring Interoperability

Even if allies and coalition partners overcome domestic obstacles to developing military capabilities based on disruptive and emerging technologies, the use of these systems can still complicate the decision-making process and pose major interoperability challenges for multinational coalitions. These challenges can complicate multinational joint operations and jeopardize the cohesion between security partners. Decision making among allies is often characterized as a complex coordination game. Although allies share a set of goals and objectives, each state sustains its own national interests. The negotiations required to harmonize these divergent political interests may result in longer time for making decisions at strategic level. The rapid rate at which information is produced and operations are conducted today can strain alliance decision-making processes. NATO's current

decision-making structure, for example, challenges the 32-member North Atlantic Council to debate and vote on matters related to the use of force. As emerging technologies accelerate the speed of war, decision-making timelines must be compressed, and alliance leaders may find themselves making decisions without the luxury of extended debate. At the operational and tactical levels, the increased deployment of military systems based on disruptive and emerging technologies has the potential to complicate interoperability among alliance forces.

As new weapon systems are introduced in the battlefield, they must be able to communicate and integrate both with each other and with older generations of weapons, and it can be a complicated task for political and technical reasons. Politically, states may be hesitant to share military and intelligence data, even with close allies. They may fear that providing unfettered access to data risks revealing sensitive sources and methods, which could cause mistrust, strain political relations or compromise ongoing military operations. Even if allies are willing to share data, significant technical hurdles remain. A lot of military and intelligence data are stored in classified national networks that are not typically designed to allow easy information sharing, and this aspect will become more pronounced as data requirements increase in an age of warfare based on emerging technologies.

Conclusions

States acquire and develop new military technologies to gain a battlefield advantage, increase operational efficiency and reduce operational risk. Although these technologies can help shift the balance of power, the armed forces often have difficulty integrating new equipment and procedures into their existing force structure because of a combination of technical and institutional barriers. The challenge of integrating new technologies into military operations is amplified in the case of multinational alliances and coalitions. While the members of these entities share security interests, each pursues its own national interests and has its own set of priorities and procedures for action. As a result, each state may have different views on how and when to use these new technologies, complicating the planning as well as the execution of military operations. However, in the case of functional

alliances and coalitions, decision-makers can always identify solutions so that such divergences can be overcome, and disruptive and emerging technologies can profoundly transform the management of multinational joint operations, making them more efficient, faster and better coordinated.

Such a solution is the conduct of joint training activities, through joint multinational exercises, not only at the command level but also with troops. The Joint Forces Command, as the only structure in the Romanian Armed Forces capable of planning and managing joint operations, is responsible for coordinating such activities on the national territory.

ROMANIAN
MILITARY
THINKING

THEORIES, MODELS AND CONCEPTS OF MISSION COMMAND

Rear Admiral Cornel COJOCARU, PhD Candidate
Commander of Romanian Fleet, Naval Forces General Staff
10.55535/RMT.2024.3.1

This approach proposes an introspection within the existing theories and models that address the concept of Mission Command (MC) to identify the place and role within the operational art, capturing the essence of the concept by examining its emergence, development and applicability. The evolution of the risks and threats to the current security environment determines a conceptual adaptation regarding the approach of the mission command, starting from the basic principles of the concept and up to the ways of its application.

The mission command concept embodies a command-and-control philosophy that is based on mutual trust between commanders at different command levels. In this approach, we start from the premise that the essence of this concept has not only theoretical but also practical significance, related to the technological evolution, the doctrinal knowledge, the general strategy, elements that define the conduct of modern armed forces.

The first objective is oriented towards identifying the particularities of the concept from its emergence to its applicability, in relation to the principles underlying it and from the perspective of existing theories and concepts. The second objective is to identify command and control models and mission command perspectives within the theoretical approaches to these concepts.

The result of the endeavour will be able to predict that the concept of Mission Command can be imposed as a basic doctrine, representing a flexible and decentralized approach to the conduct of military actions at any level of military art.

Keywords: mission command; control; leadership; auftragstaktik; indirect approach;

INTRODUCTION

The purpose of this article is to identify the place and role of the *Mission Command/MC* concept within the operational art, through considering existing theories and models, capturing the essence of the concept by examining its emergence, evolution and applicability.

Beyond the concept it represents, *Mission Command* means adopting mission-focused/tailored action decisions that today define a battlefield command model. While it can be suggested that this is a concept applicable only at the tactical level, the usefulness of application at the strategic level will be highlighted by identifying both the role and the influence it can have on the fulfilment of the mission at the operational or tactical level.

The concept has its modern origin in Prussian doctrine, but it can be said that the vein of its application is found in the first writings of the military strategy approach[1], within the *Art of War* (Sun Tzu, 2012) and within the current principles (DAR, 2012, p. 21)[2] of the use of armed forces in military actions, today the concept representing the essence of the application of modern operational art through concrete actions.

The "mission command" concept consists of centralized command exerted from the central level and decentralized execution based on decision in the battlefield, speed of reaction, freedom of action, initiative and efficiency.

The *mission command* concept consists of centralized command exerted from the central level and decentralized execution based on decision in the battlefield, speed of reaction, freedom of action, initiative and efficiency. In all these cases, information is the basic pillar in the analysis of the existing situation observed by the battlefield commander, in relation to the desired situation provided in the intention of the higher commander.

The evolution of the risks and threats to the current security environment determines a conceptual adaptation regarding the approach to the *mission command*, starting from the basic principles of the concept and up to the ways of its application.

[1] See Helmuth von Moltke Sr. (1800-1891); Otto von Moser (1860-1931). *Ausbildung und Führung des Bataillons, des Regiments und der Brigade. Gedanken und Vorschläge. Mittler-Verlag. Berlin 1914*; Hervé Coutau-Bégarie (1956-2012). *Tratat de strategie,* vol. I, 2006, București: Editura Universității Naționale de Apărare. (A.N.)

[2] Initiative, surprise, morale keeping (A.N.)

The *mission command* concept embodies a command-and-control philosophy that is based on mutual trust between commanders at different command levels. In this philosophy, as well as from the point of view of modern operational art, the mission command is materialized by the independent execution of the orders by the lower echelon commander, an action that is based on a common understanding of the higher commander's intention. Thus, the concept is used to empower subordinate commanders to make decisions and act by applying the principles of actionable leadership without going outside the legal framework of the mission received.

The "mission command" concept is used to empower subordinate commanders to make decisions and act by applying the principles of actionable leadership without going outside the legal framework of the mission received.

The essence of this concept encompasses not only a theoretical meaning but also a practical one, related to technological evolution and doctrinal knowledge, to the general strategy, elements that define the conduct of the modern armed forces.

The first objective of this article is oriented towards identifying the particularities of the concept from its emergence to its applicability, in relation to the principles underlying it and from the perspective of existing theories and concepts. The second objective is to identify command and control models and the *mission command* perspective within the theoretical approaches to these concepts.

It can be foreseen that this concept can impose itself as a basic doctrine in the spectrum of modern leadership application models, representing a flexible and decentralized approach to the leadership of military actions at any level of military art. Thus, at the strategic level, the concept embraces a specific philosophy that has its essence in the school of thought of the current military leaders and is based on a specific national culture, aligned with the Euro-Atlantic allied commitments.

MISSION COMMAND – BETWEEN EMERGENCE AND APPLICABILITY

From the early stage of expressing this concept, it can be seen that the flexibility and adaptability of actions on the battlefield are characteristics of the mission command philosophy. Sun Tzu presented, in his work, the role of the lower-level commander to make decisions adapted to the situation in the battlefield, depending on the reaction of the enemy, *"success in warfare is gained by carefully accommodating*

ourselves to the enemy's purpose" (Sun Tzu, ib., p. 49). It can thus be pointed out that, beyond the existence of the concept, its essence has been captured since the beginnings of military art.

The evolution of the concept was marked by the evolution of military art through the scientific footprint inherited from Helmuth von Moltke, Carl von Clausewitz, Antoine Henri Jomini, Otto von Moser, Hervé Coutau Bégarie etc.

The concept was used at an early stage in the form of mission orders by the Prussian army under the name *"Auftragstaktik"* (Gunther, 2012). Subsequently, the concept was adopted and applied by Field Marshal Helmuth von Moltke Sr. who predicted that a lower-level commander must know the purpose and desired end state of an operation. These two elements represented two determining components of the upper-level commander's intention. Moltke suggested that between the purpose and the end state there are certain conditions to be fulfilled, which a commander must fulfil by any means and by adapted, intuitive and applicable decisions (Ib., p. 8).

The *"Blitzkrieg"* concept (Frieser, 2010) is the obvious result of the practical evolution of the *"Auftragstaktik"* concept, the latter being successfully applied by Germany during the Second World War when tactical-level commanders were granted the autonomy of action to respond effectively to the volatility of the conditions in the battlefield. Subsequently, this freedom of action of commanders was restricted by decisions at the strategic level, which led to multiple defeats of Nazi Germany (Deighton, 1981). The concept of *"Auftragstaktik"* has attracted the attention of theorists in the US Army being intensively studied, so that in the American doctrine (FM 100 5 Operations, 1986; 1993; Joint Doctrine, 2007), under the concept of *Mission Orders*, certain specific characteristics can be identified that today define the concept of *Mission Command*, namely actionable intensity, flexibility and confidence in the initiative of commanders, decision speed, clearly defined objectives, effort concentration.

The "Blitzkrieg" concept is the obvious result of the practical evolution of the "Auftragstaktik" concept, the latter being successfully applied by Germany during the Second World War when tactical-level commanders were granted the autonomy of action to respond effectively to the volatility of the conditions in the battlefield.

The modern concept of *Mission Command* [AJP 01(D) Allied Joint Doctrine, 2010] is found for the first time in AJP 01(D) Allied Joint Doctrine, 2010 edition, summing up principles such as *"freedom of action, efficiency, opportunity"* (Ib., p. 6 3). In 2012, in ADP 6-0 (Army Doctrine Publication), the *mission command* concept summed up confidence in the self and in subordinates, mutual understanding,

the commander's intention, clear mission orders, initiative, discipline, accepted risks. These are characteristics of the mission command that are stipulated in the documents as principles, as follows: *"Competence, Mutual trust, Shared understanding, Commander's intent, Mission orders, Disciplined initiative, Risk acceptance"* (ADP 6-0 Mission Command, HQ Dept. of Army, p. 2). The 2017 version of AJP 01(D) Allied Joint Doctrine introduces principles such as initiative, speed of action, in relation to the intention of the higher commander and the tasks received by action order.

The influence of modern operational art is felt in AJP 01(F) Allied Joint Doctrine, 2022 edition, the essence of the *mission command* concept being the compliance with the intention of the higher commander and the fulfilment of the tasks by any means, as the *"commander's primary responsibility*" [AJP 01(F) Allied Joint Doctrine, NSO, 2022, p. 84]. In this manual, the concept can be identified as follows: *mission command "shapes the command styles, attitudes and behaviours of commanders and subordinates. It is based on empowered leadership, which enables decisions to be made by those best placed to make them, exploiting opportunities that emerge from competition. Mission command offers a significant advantage when applied correctly, enabling the joint force to overcome a rival in the most chaotic and demanding circumstances by maximizing initiative to seize opportunities*" (Ib.).

Mission command "shapes the command styles, attitudes and behaviours of commanders and subordinates. It is based on empowered leadership, which enables decisions to be made by those best placed to make them, exploiting opportunities that emerge from competition".

Summing up these defining elements of the concept, it can be formulated that, in a modernist sense, the essence of the *mission command* is based on modelling, command style, attitudes and skills, leadership, initiative, opportunity, and the list of principles can continue. However, to outline the overall picture, further we will consider some theoretical approaches to the concept of *mission command* from its emergence to modern times.

THEORIES AND APPROACHES TO THE MISSION COMMAND CONCEPT IN MILITARY STRATEGIC THINKING

Sun Tzu, in his masterpiece *The Art of War* (2023), emphasizes the flexibility, adaptability and wise use of initiative in military actions. Even if we do not find the *mission command* concept explicitly stipulated and defined as such, Sun Tzu's approach, by promoting these principles, promotes a similar philosophy, highlighting

how important is the freedom of action of the lower-level commanders on the battlefield in achieving victory and establishing the outcome of the battle. Sun Tzu emphasizes the role of information, surprise and adaptability, these principles being part of the essence of the *mission command* concept.

Carl von Clausewitz, in his work *On War* (1932), highlights some perspectives that can be interpreted in terms of *mission command* principles. It emphasizes the freedom that provides certainty regarding the morale of the troops in conditions of uncertainty related to the evolution of the unpredictable situation on the battlefield compared to the dynamics and complexity of the conflict, elements of the presented concept.

Carl von Clausewitz, in his work "On War", highlights some perspectives that can be interpreted in terms of "mission command" principles. It emphasizes the freedom that provides certainty regarding the morale of the troops in conditions of uncertainty related to the evolution of the unpredictable situation on the battlefield compared to the dynamics and complexity of the conflict, elements of the presented concept.

Antoine Henri Jomini, a theoretician of the art of war, had his own perspective on what military strategy means. His approach can be also analysed through the prism of the mission command concept. Jomini stressed the importance of the lines of operations, which force the commanders to focus on the decisive conditions of an operation and to have the initiative to choose exactly the decisive point, corresponding to culmination of the battle, which can be seen as the freedom of action promoted by the *mission command*. It should not be overlooked that Jomini promoted a very well-defined command structure where freedom of decision could be oppressed at any time.

Helmuth von Moltke, a coordinator of the application of the *Auftragstaktik* concept in the Prussian army, foresaw that it was hard to predict all the variables on the battlefield. He promoted the need for a degree of autonomy in decision-making by subordinate commanders, which can be associated with the essence of the *mission command* concept.

Tayer Alfred Mahan, even if concerned with the importance of controlling the seas and the projection of American naval power on the seas and oceans of the world, also touched, along with the naval strategy, elements of command and control of forces, direct conduct of forces, their mobility, autonomy of command, initiative etc. In this context, Mahan stressed the importance of giving ship and fleet commanders the freedom to exploit opportunities in accordance with the mission objectives set by the higher commander (Mahan, 1890).

John Boyd, author of the OODA Loop (*Observation, Orientation, Decision, Action*) concept, offered a model of short-term decision-making

adaptable to the dynamics of military action to gain a tactical advantage over the adversary. Boyd promoted adaptability, initiative and the ability to make quick and effective decisions by supporting the decentralization of conducting forces, aspects that also converge towards the philosophy of *mission command*.

Julian Corbett, as a military strategist, captured the principles of the *mission command* concept in a wider context, especially in terms of encouraging coordination and adaptability of forces to the dynamics of actions in the theatre of maritime operations. He was adept at the complementarity of land and naval forces at the seaside, demonstrating an overall vision of centralized leadership. Being a supporter of strategic flexibility, Corbett became the first supporter of freedom of action promoted from the strategic, political and military levels (Corbett, 1911).

Basil Liddell Hart was a military historian and theorist who developed the concept of indirect approach in the dialectic of the art of war compared to the direct approach concept stating that "in strategy, the longest way round is often the shortest way home. A direct approach to the object exhausts the attacker and hardens the resistance by compression, where as an indirect approach loosens the defender's hold by upsetting his balance".

Basil Liddell Hart (2022) was a military historian and theorist who developed the concept of *indirect approach* in the dialectic of the art of war compared to the *direct approach* concept stating that *"in strategy, the longest way round is often the shortest way home. A direct approach to the object exhausts the attacker and hardens the resistance by compression, where as an indirect approach loosens the defender's hold by upsetting his balance"* (Liddell Hart, 1991). In essence, *indirect approach* and *mission command* share the principle that success in operations is not always based on direct confrontation and brute force, but on the agility, innovation and ability to exploit the opponent's weaknesses. Liddell Hart advocated a leadership that allows great freedom of manoeuvre and initiative, aspects that are fundamental in *mission command*.

Colin S. Gray[3], in his professional training as a contemporary security and strategy theorist, highlighted the complexity of modern conflicts and promoted the permanent adaptation of military doctrines to the current realities. Even if he did not explicitly address the concept of *mission command* at the level of his perspective as a strategist, he emphasized the importance of flexibility, adaptive strategic thinking

[3] Colin S. Gray, (1943-2020), Professor of International Relations and Strategic Studies at the University of Reading, UK, was an advisor on defence issues in the US and UK governments. Author of the works: *Modern Strategy* (1999), *Strategy and History: Essays on Theory and Practice* (2006), (A.N.).

and organizational culture while supporting innovation and initiative at the lower-level echelons through promotion at the strategic level. This approach affirmatively calls for the promotion of the dynamic and responsive approach in operational and tactical military leadership styles.

The result of the analysis of the theoretical approach, directly or indirectly, in the main works that develop or capture the *mission command* concept in its evolution, reveals that it has reached a maturity that captures all facets of the command-and-control tool of a military leader at any level of military art. However, the essence it embodies at each strategic, operational and tactical level is the subject of a separate study generated by the very complexity of the ways of using this command-and-control tool.

MISSION COMMAND – A MODEL OF COMMAND AND CONTROL

In order to determine the command-and-control characteristic of the *mission command* and to identify an optimal model to use it as an established conduct tool, some existing command and control models in the military domain will be analysed in comparison with management models in the civilian field of leadership in order to capture certain advantages and limitations of the concept. Command and control models such as authoritative, participatory or delegative command will be considered [direct/authoritarian command, control-based command, detailed command vs. management by objectives (MbO) (*Sisteme, metode* şi *tehnici de management*, 2015, p. 630) and management by delegation (MbD) (Ib., p. 64)].

Direct/authoritative command is a type of command and control in which the commander directly orders the tasks, objectives and the manner of execution of the mission without consulting subordinates.

Direct/authoritative command is a type of command and control in which the commander directly orders the tasks, objectives and the manner of execution of the mission without consulting subordinates. They are less involved in the decision-making process and have the role of executing the orders received exactly. Deviations are not allowed, the effect being a rigid organizational structure, a demoralizing and demotivating work environment. Such a model limits the innovation and performance of subordinates. With all these disadvantages, the model lends itself to being used at the lower tactical level of command, at the execution structures of team level, detachments etc.

Control-based command is an authoritative command model similar to the previous one, but which involves strict monitoring and control over the activities performed by subordinates. The commander controls the execution of tasks and objectives, pursues the fulfilment of decisive conditions and creation of effects. Its decisions are made centrally, based on reports and information updates received from subordinates. Decisions are based on pre-established projects, plans or procedures where innovation, initiative, adaptation to unforeseen events do not take place. Despite the disadvantages, this model is sometimes suitable for use at the higher tactical command level, respectively at the level of battalion, regiments etc.

Detailed command is characterized by principles such as centralized control, specific and detailed orders, rigorous coordination, efficient and accurate communication, synchronization etc. Under this model, decisions are made at higher levels of command and are passed on to subordinates in the form of detailed orders. The main characteristics of this type of command can be detailed planning, efficient and accurate communication, supervision, monitoring etc. This approach ensures the transmission of all command-and-control elements established through an operational design so that all phases of an operation are strictly coordinated and aligned with its objectives and in accordance with the intention of the higher-level echelon.

Detailed command is characterized by principles such as centralized control, specific and detailed orders, rigorous coordination, efficient and accurate communication, synchronization etc. Under this model, decisions are made at higher levels of command and are passed on to subordinates in the form of detailed orders.

The detailed command is mainly used in situations where the risks are high and the effects of the action are of great importance. Such a model can be found at the operational and strategic level, especially in operations involving inter-agency coordination. A specific field of application is that of logistics because logistics support operations are complex, so a deviation from the plan can have significant undesirable effects.

By comparison, the *mission command* style offers more flexibility and speed in response while previous models offer tighter control and precision. The choice between these models depends on the nature of the mission, the operational environment and the degree of risk accepted by the commander.

At the same time, there are similarities between *mission command* and other concepts in the civilian field of leadership that value flexibility and adaptability, such as management by objectives (essentially participatory) and management by delegation. These approaches

recognize the importance of setting clear objectives but allow team members to find the best ways to achieve those objectives.

The essential peculiarity of *mission command* is that this concept is deeply rooted in the military field. The need to increase trust and initiative in situations of uncertainty and high risk that higher commanders must grant to lower-level commanders can be observed: *"Commanders who delegate authority to subordinate commanders need to state clearly their intentions, freedoms and constraints, designate the objectives to be achieved and provide sufficient forces, resources and authority, required to accomplish their assigned tasks"* (COPD, v 3.0, 1.10, pp. 1-12).

CONCLUSIONS

In general, the evolution of the *mission command* concept reflects a paradigmatic adaptation influenced by the strategic direction, the operational thinking and the evolution of the tactical situation moving from a centralized and hierarchical model to one that highlights adaptability, innovation and accountability at all three levels of military art.

"Commanders who delegate authority to subordinate commanders need to state clearly their intentions, freedoms and constraints, designate the objectives to be achieved and provide sufficient forces, resources and authority, required to accomplish their assigned tasks".

It can be accepted that *Auftragstaktik*, the Prussian concept, is the precursor of the concept of *mission command* in its original form, and with the development of operational art, it has reached a level of coagulation that covers a wide range of principles and peculiarities, keeping the essence of the concept.

The new conceptual approach to *mission command* arose as a reaction to the rigidity and limitations of traditional command and control systems characterized by a manifest inhibition of individual initiative and a lack of freedom of decision, including inadequacy to the battlefield situation.

Today, we can speak of a reality favourable to the manifestation of a modern concept adapted to the principles of operational art, technological evolution, dynamic characteristics of the battlefield, as well as to training and leadership of the command act.

At the strategic level, the *mission command* provides an appropriate framework to promote the agility and adaptability of the decision-making process at the military level and the formulation of directives in the spirit of encouraging creativity based on the experience and critical thinking of the operational-level commander. This approach

facilitates the development of command-and-control culture, the personal development of leaders thus increasing the self-confidence of commanders.

At the operational level, the *mission command* promotes flexible and adaptable ideas to the security environment and the dynamics of operations, is based on the sense of cohesion and provides a high degree of dignity to the commanded commanders and forces.

At the tactical level, the *mission command* promotes decision-making autonomy in relation to the information flow and the dynamics of military actions, encourages the initiative on the battlefield in order to achieve the objectives at the operational level by fulfilling the tasks of the mission at the tactical level.

The "mission command" represents the foundation of the operational art through realistic adaptive approaches to the management of the combat forces, in relation to the evolution of the security environment, with the existing risks and threats, so that, from the military conduct point of view, the philosophy of the concept responds to the needs and challenges of the future war.

The result of the analysis of the conceptual content of the *mission command* highlights that it combines flexibility, adaptability, initiative and understanding, giving higher commanders the opportunity to invest confidence and empower inferior commanders to maintain strategic direction, perform tasks and achieve the overall objectives of the mission by producing action-friendly effects.

From the point of view of execution and in relation to the command and control of the action, the *mission command* essentially means centralized conduct and decentralized execution. It can be mentioned that the modern approach to the concept contrasts with traditional leadership styles, such as centralized command and control, where decisions are made by the higher-level echelons, structured and transmitted rigidly, thus limiting the ability of the lower commanders to respond quickly to changes in the area of operations.

Today, the *mission command* represents the foundation of the operational art through realistic adaptive approaches to the management of the combat forces, in relation to the evolution of the security environment, with the existing risks and threats, so that, from the military conduct point of view, the philosophy of the concept responds to the needs and challenges of the future war.

The promotion of this concept is a permanent concern requiring a doctrinal adaptation, from the conceptual point of view, and the promotion of a flexible, adaptable and efficient approach in the management of military operations, from the actional point of view.

BIBLIOGRAPHY:

1. ADP 6-0 Mission Command, HQ Dept. of Army (2014). Washington D.C., https://armypubs.us.army.mil/doctrine/index.html, retrieved on 12 May 2024.
2. AJP 01(D) Allied Joint Doctrine (2010, 2022), https://www.gov.uk/government/publications/ajp-01-d-allied-joint-doctrine.pdf, retrieved on 12 June 2024.
3. COPD/The Comprehensive Operations Planning Directive (2010), v 3.0, 1.10. Belgium, https://www.google.com/search?client=firefox-b-d&q=COPD%2FThe+Comprehensive+Operations+Planning+Directive%2FDirectiva+pentru+planificarea+cuprinz%C4%83toare+a+opera%C8%9Biilor%2C+v+3.0%2C+1.10, pdf, retrieved on 2 June 2024.
4. Corbett, J. (1911). *Some Principles of Maritime Strategy*. London: Longmans, Green and Co.
5. Coutau-Bégarie, H. (2006). *Tratat de strategie*, vol. I. București: Editura Universității Naționale de Apărare.
6. Deighton, L. (1981). *Blitzkrieg: From the rise of Hitler to the fall of Dunkirk*. Grafton.
7. Doctrina Armatei României/Doctrine of the Romanian Armed Forces (2012). București: Statul Major General.
8. FM 100-5 Operations (1993). Washington D.C., https://en.wikipedia.org/wiki/Field_Manual_100-5, pdf, retrieved on 21 May 2024.
9. Frieser, K.H. (2010). *Mitul Blitzkrieg-ului. Campania din Vest a Wehrmacht-ului, 1940*. București: Editura Militară.
10. Gray, C.S. (1999). *Modern Strategy*, Oxford University, https://global.oup.com/academic/product/modern-strategy-9780198782513?cc=ro& lang=en&, retrieved on 12 May 2024.
11. Gray, C.S. (2006). *Strategy and History: Essays on Theory and Practice*. London and New York: Routledge.
12. Gunther, M. (2012). *Auftragstaktik: The Basis for Modern Military Command?* Fort Leavenworth, Kansas: School of Advanced Military Studies United States Army Command and General Staff College.
13. Liddell Hart, B.H. (1991). *Strategy*, 2nd ed. revised. New York: Meridian.
14. Liddell Hart, B.H. (2022). *Strategy: The Indirect Approach*. Legare Street Press.
15. Mahan, T.A. (1890). *The Influence of Sea Power upon History*, 1660-1783. Boston.
16. Moser, von O. (1914). *Ausbildung und Führung des Bataillons, des Regiments und der Brigade*. Berlin: Gedanken und Vorschläge. Mittler-Verlag.
17. *Sisteme, metode şi tehnici de management*, lecture notes (2015). București: Editura Universitaria.
18. Sun Tzu (2012). *Arta Războiului*. București: Editura Antet Revolution.
19. Sun Tzu (2023). *Arta Războiului/The Art of War*. București: Editura Litera.

ROMANIAN
MILITARY
THINKING

DOCTRINAL CONSIDERATIONS ABOUT THE SEABED WARFARE

Professor Lucian Valeriu SCIPANOV, PhD

Naval Forces Department, Command and Staff Faculty,
"Carol I" National Defence University, Bucharest

Marian-Vasile SAVA, BEng

Romanian Naval Forces

10.55535/RMT.2024.3.2

The present paperwork provides an intrinsic examination of the seabed environment and intends to identify the opportunity to integrate the seabed warfare concept into the naval doctrine. The objective of this endeavour is to determine the place of seabed warfare in the doctrine. In addition to the clarification, some amendments to the Romanian naval doctrine are suggested in order to improve the doctrinal content regarding underwater warfare and seabed security. To that end, it is conducted a comparative analysis between different naval allied doctrines, some leading global technology corporations, and non-governmental organizations. The result of the research should support the development of a robust naval doctrine, adapted to technological advances and the tactics of using modern weapons specific to seabed warfare. Moreover, upgrading the content of a maritime security strategy, which would contain measures in critical areas such as submarine communications, energy exploitation and the use of underwater vehicles, represents a direction to follow, especially in the conditions of multi-domain actions that have effects on the maritime environment.

Keywords: seabed warfare; naval doctrine; maritime control; underwater operations; underwater critical infrastructure;

INTRODUCTION

In the framework of maritime security, this paperwork provides an intrinsic examination of the seabed environment and intends to identify the opportunity to integrate the *seabed warfare* concept into the Romanian Navy doctrine.

The underwater dimension is becoming increasingly competitive, contested, and to some extent congested, and represents a distinct challenge not only for Navies but indeed for the combination of military and civilian, public and private entities that contribute to pursuing any country's economic and strategic interests.

The underwater dimension represents a distinct challenge not only for Navies but indeed for the combination of military and civilian, public and private entities that contribute to pursuing any country's economic and strategic interests.

This scientific approach is based on the premise – previously launched by the authors, in a specialized publication – that *"the security of the seabed is a component of maritime security that requires a more detailed control of the underwater environment"* (Scipanov, Sava, 2024). A perspective of controlling the seabed has been considered through active and passive measures, both in the military and civil domain, through the participation of the entrepreneurial environment and ecological organizations, in order to safely exploit the maritime infrastructure, mainly civilian and military critical infrastructure.

The first objective of this endeavour is to determine the place of seabed warfare in the present doctrine. This aspect is strengthened by a comparative analysis of some doctrinal approaches from the perspective of some international actors, active in the maritime field. The arguments presented will support the place and role of seabed warfare in a national doctrine approach that will be able to open opportunities for the development of capabilities in the naval field.

The second objective is to provide some amendments to the Romanian naval doctrine to improve the doctrinal content regarding underwater warfare and seabed security. To effectively integrate

seabed warfare into naval doctrine, three directions of action in the Romanian Navy are proposed. The analysis will allow the identification of some particularities from a tactical perspective, thus ensuring content elements regarding their significance and some implementation possibilities.

The result of the research should support the development of a robust naval doctrine, adapted to technological advances and the tactics of using modern weapons specific to seabed warfare. It is envisioned to take into account the military field contribution to maritime security as well as the participation of civil institutions, governmental and non-governmental organizations, specialized companies, and ecological associations in this endeavour. Thus, the field of seabed security will be able to complete the component spectrum of the maritime security cluster.

We start from the premise that the direction of action for the modern Romanian naval forces in strengthening maritime security, implicitly the submarine environment, will also be found in the structural model of a maritime security strategy for the Black Sea, in line with the construct of comprehensive strategies.

INTEGRATION OF THE SEABED WARFARE INTO THE DOCTRINE

In this chapter, certain amendments will be presented in order to improve the doctrinal content by identifying the importance of the *seabed warfare* from an operational and tactical planning perspective. We start from the premise that the direction of action for the modern Romanian naval forces in strengthening maritime security, implicitly the submarine environment, will also be found in the structural model of a maritime security strategy for the Black Sea (Scipanov, 2020, pp. 68-97), in line with the construct of comprehensive strategies. To effectively integrate *seabed warfare* into our doctrine, certain Romanian Navy contributions will be identified in this section and organized into three distinct functions. Additionally, tactical insights for each function will be provided, ensuring a comprehensive understanding of their implementation and significance. This structured approach will not only streamline the integration process, but also offer the directions to enhance naval capabilities by addressing the unique challenges and opportunities associated with *seabed warfare*. Through this method, the Navy will be better ready to harness the full

potential of seabed operations, ensuring robust defence and control in this critical domain.

To ensure that the Romanian Navy can achieve its maritime control objectives, it is necessary to establish a classification system for *seabed warfare* operations and a corresponding operational framework. These operations include all activities performed by the Navy or on its behalf, involving the seabed, whether conducted from, to, or directly on it.

Seabed warfare operations support the freedom of information, access, and action for our naval forces, as well as the protection of our critical infrastructure, and maybe the most important aspect is that the *seabed warfare* is a crucial piece of the broader maritime control. These operations involve the implementation, deployment, and utilization of fixed, semi-fixed, or mobile underwater capabilities that can operate towards, from, and on the seabed, either independently or within a network. They ensure the freedom of action for our Navy, protect our submarine installations (including submarine communication cables), and safeguard our national interests related to the exploration and exploitation of mineral and energy resources. Additionally, these operations can pose a credible threat to any potential enemy forces that might target our national interests.

Seabed warfare operations support the freedom of information, access, and action for our naval forces, as well as the protection of our critical infrastructure, and maybe the most important aspect is that the seabed warfare is a crucial piece of the broader maritime control.

Considering the diverse, evolving, and potentially dual nature of underwater operations, seabed warfare activities are encompassed within a broader strategy of maritime area control. They are crucial to our national ambition to maintain our capacity for early warning, action, and contribution to national resilience.

A comparative analysis of specialized studies and different approaches of other *seabed warfare* doctrines is compulsory to complete the research objectives. The result will give an image of the interested actors in maritime security when they promote, achieve, or develop *seabed warfare*.

For example, the focus of the UK seabed warfare doctrine goes towards the seabed cables (Brooke, 2023). UK *seabed warfare* broadly refers to undersea warfare in which the seabed is the focus. Undersea warfare is not a new concept, but it is also a concern since submarines

have long played a vital role in the Royal Navy's history. What is new, or at least becoming more widely discussed in public, is the growing threat to critical infrastructure on the seabed and the resulting risk to national security. *Seabed warfare* is no longer a futuristic scenario, but a contemporary form of conflict in the era of increasing geopolitical, global, and regional competition. As the ability to manoeuvre, map, and operate at greater depths increases, critical maritime infrastructure along the seabed resembles the exposed underbelly of national security in a new age of undersea warfare. The *seabed warfare* can thus be characterized as an interim phase between an era of maritime competition and security contestation.

The US defined seabed warfare as "operations that involve undersea networks and systems capable of operating on the seabed, interacting with seabed systems, and taking actions against other systems".

The US defined *seabed warfare* as *"operations that involve undersea networks and systems capable of operating on the seabed, interacting with seabed systems, and taking actions against other systems"* (Carr et al., 2018, p. XX and p. 9).

Seabed warfare utilizes seabed capabilities or systems that interact with seabed infrastructures to perform missions such as underwater warfare, submarines, mine countermeasures, surface warfare, military deception etc.

An interesting approach to seabed is that of the Italian Navy (Marina Militare Italiana – MMI) that sees it as the *"fifth physical operational domain, beside air, land, maritime and space"* (Calcagno, Marrone, 2023, p. 7). From the Italian Navy perspective, the underwater dimension, including the seabed area, is now seen as the new, challenging and physical operational maritime domain. The Navy acknowledges that *"operating underwater requires renewed attention, a novel doctrinal approach, as well as peculiar skills and technological solutions, especially considering that the use of UUVs has pushed the boundaries in terms of how deep navies as well as private actors can operate"* (Ib.).

As regards the French doctrine approach, a preoccupation concerning seabed warfare can be noted and can be underlined in France's ability to guarantee meeting its ambitions in the seabed domain. French naval doctrine defines a classification of seabed warfare

operations and establishes the framework for seabed operations. *"These operations encompass all the activities conducted by the French Ministry for the Armed Forces, or for its benefit, from, to and on the seabed (…). Seabed warfare operations include implementing, deploying, and utilizing fixed or mobile underwater capabilities able to operate towards, from, and on the seabed, either independently or in a network"* (Seabed Warfare Strategy, 2012, p. 38). In other words, these seabed operations contribute to freedom of movement, protecting critical underwater infrastructure and promoting seabed security.

The People's Liberation Army (PLA) Navy focuses on detection and early warning of underwater enemies. They are planning to build a so-called *"The Great Underwater Wall"* which is a network of stationary sensors on the ocean seabed that listen for enemy submarines and Anti-Surface Warfare efforts (Carr et al., ib., pp. 2-3). This is another indicator that underlines the concerns of the main global and regional actors in the maritime field regarding the coverage of seabed security through measures to guarantee maritime security, in general, and economic security, in particular.

The People's Liberation Army Navy focuses on detection and early warning of underwater enemies. They are planning to build a so-called "The Great Underwater Wall" which is a network of stationary sensors on the ocean seabed that listen for enemy submarines and Anti-Surface Warfare efforts.

Similarly, defence companies focus on developing unmanned underwater vehicles and advanced sensors. Kongsberg[1] considers that autonomous platform has proven itself superior to all others in this domain (https://www.kongsberg.com/maritime/about-us/news-and-media/blog-stories/seabed-warfare/). Moreover, there are companies focused on underwater sensors and detection of submarine threats (https://www.sercel.com/en/market/defense/submarine-warfare).

SAAB[2] is a company that pays a lot of attention to the submarine field and especially to the seabed domain. In recent years, dependence on subsea infrastructure has increased on a global scale. There has been a focus on subsea cables, which are vital for the global economy and for communications. *Seabed warfare* therefore involves a major

[1] Kongsberg – *"a leading global technology corporation delivering mission-critical solutions with extreme performance for customers that operate under extremely challenging conditions",* https://www.kongsberg.com/who-we-are/ (A.N.).

[2] Sweden company, serve the global market with world-leading products, services and solutions from military defence to civil security, https://www.saab.com/. (A.N.).

risk of sabotage to subsea infrastructure. Many countries are investing in their own deep-water capacity to respond to current and future threats, known as *seabed warfare*. Remotely operated underwater systems are generally used for payload transportation, observation, surveillance, and mine-clearing (https://www.saab.com/markets/norway/editorial-articles/seabed-warfare).

This increase is also due to rising demand for stealth seabed warfare systems and the growing use of AUVs for deep sea warfare. *"There is a real and present threat out there today"* (Lade, 2022). Technological development determines the adaptation of operating systems on the seabed, the underwater environment being a dimension that should not be omitted.

Some international actors' actions are causing concerns at the level of seabed security. For example, it can be stated that Russia is "the most capable nation to conduct seabed operations today".

Some international actors' actions are causing concerns at the level of seabed security. For example, it can be stated that Russia is *"the most capable nation to conduct seabed operations today"* (Ib.). It is possible to observe the concern regarding the effects that the uncontrolled or unsupervised actions of some international actors possessing combat capabilities on the seabed can produce. The lack of reaction is not a proper attitude to the threat to the seabed security. *"They do seabed operations, and that's a range of things. They can lay sensors, they can interdict other people's infrastructure, they can survey, they can do the whole gambit of what you might want to do on the seabed. So, there is a real and present threat out there today",* underline Chris Lade, too (Salerno-Garthwaite, 2022). If specialists in the field mention these aspects, it requires great attention to be given to the field of seabed security. It confirms the purpose of our approach to highlight the importance of the analysed domain.

Sercel[3] participates in the design and manufacturing of detection and measurement systems for submarines and marine drones. Undersea warfare consists of operations conducted to establish battlespace dominance in the underwater environment. The *undersea*

[3] Sercel is part of Viridien Group. Sercel is the world's leading designer and manufacturer of high-tech solutions for subsurface exploration, https://www.sercel.com/en. (A.N.).

warfare market is characterized by the reduction in noise levels of modern submarines, as well as the widening and shifting of conflicts to shallow areas. It necessitates the development of more advanced sensors and detection systems to ensure state sovereignty (https://www.sercel.com/en/market/defense/submarine-warfare).

Sercel is an example of a company concerned with the development of underwater capabilities, for the exploitation of underwater resources. It also contributes to monitoring underwater activities, being an important actor in the field of innovation. The presence of underwater technology on the market highlights the need to promote the underwater field and draws attention to the inherent development of seabed warfare as well as to the navies concern to develop capabilities in the field.

The presence of underwater technology on the market highlights the need to promote the underwater field and draws attention to the inherent development of seabed warfare as well as to the navies concern to develop capabilities in the field.

Considering the example of other states and the increased importance of the underwater domain, Romanian Navy should consider to give attention to this subject. For an effective maritime security, we propose some amendments to the Romanian naval doctrine. Our proposal is to introduce the concept of *seabed warfare* and to organize it around three main functions:

- *gain seabed expertise;*
- *conduct seabed surveillance;*
- *execute seabed operations.*

To achieve the outlined objectives, we will elaborate on each of the three previously mentioned functions. This analysis will provide a clear framework for understanding how each function contributes to *seabed warfare* goals. Breaking down these functions and exploring their roles, operational mechanisms, and tactical applications, valuable insights will be presented into their importance and interconnectivity. This approach will ensure that we not only meet but also exceed the proposed objectives, paving the way for a robust and effective implementation of our vision in a future maritime security for the Black Sea (Scipanov, 2020).

Gain seabed expertise

This function must enable the measurement, characterization, and analysis of the seabed and underwater environment physical properties. This function could include:

- Hydrographic and oceanographic missions involve the comprehensive collection, analysis, and storage of critical data, including bathymetric surveys and gravimetric measurements, essential for the safe navigation of underwater vehicles and the autonomous operations of naval forces. These missions also utilize magnetometry in order to identify magnetic anomalies and characterize the seabed, which is vital for managing acoustic sensors at ultra-low and very-low frequencies. Additionally, they assess velocity profiles, ambient noise levels, and environmental transparency (Metrick, Weinberger, 2016, p. 42). Depending on the level of confidentiality required or the permissiveness of the data collection environment, these operations can be executed using sovereign military resources, through collaborations with NATO/EU allies, or with trusted partners. This type of operation can be carried out by specialized structures in the field of maritime and fluvial hydrography using MUVs and ROVs or other sensors launched from specialized platforms.
- Mine warfare sounding survey missions are conducted to ensure a comprehensive understanding of the seabed. These data collection operations enhance the effectiveness of mine warfare strategies during both peacetime and crises, supporting deterrence, safeguarding critical infrastructure, and enabling the intervention of air-maritime forces.
- Special rapid environmental assessment missions in disputed areas aim to discreetly penetrate underwater into the depths of an enemy's territory. The goal is to collect crucial geographical, hydrographical, oceanographic, and meteorological information needed to plan special naval actions or amphibious operations in strategic ports or areas. These missions seek to obtain a detailed understanding of environmental data in non-permissive environments, including the underwater volume and coastal zone. Usually, such operations are performed by special operation forces launched from submarines or using MUVs, depending on the complexity.

Hydrographic and oceanographic missions involve the comprehensive collection, analysis, and storage of critical data, including bathymetric surveys and gravimetric measurements, essential for the safe navigation of underwater vehicles and the autonomous operations of naval forces.

Conduct seabed surveillance

This type of operation can be described as passive activity because only fixed or mobile sensors are used. Seabed operations related to seabed surveillance (Ib., p. 19) include:

- Monitoring the seabed environment and critical submarine infrastructure (communication cables, natural gas platforms etc.) within our maritime area of interest (territorial waters and EEZ) and in any area or theatre of operations.
- Observing the submarine environment from the seabed by deploying and utilizing underwater detection systems like seabed sensor nets to secure the operational area and support the navy ops or early warning.
- This type of surveillance can be considered to be attributed to the specialized electronic warfare and observation structures by implementing a seabed surveillance network (Scipanov, Nistor, 2019). In this manner, the Recognized Maritime Pictures (RMP) will be complete.

To bolster surveillance efforts, targeted investigations must be feasible upon initial detection or indication of a threat, preceding any force using operations.

Execute seabed operations

The range of activities linked with the seabed operation function encompasses:

- Searches and inquiries conducted to resolve potential uncertainties, identify threats, and, if needed, prepare for underwater interventions. To bolster surveillance efforts, targeted investigations must be feasible upon initial detection or indication of a threat, preceding any force using operations.
- Intervention to neutralize devices that may jeopardize the operational freedom of our naval forces or critical infrastructure.

- Search and recovery operations targeting sensitive objects containing vital information, such as missile debris or flight recorder black boxes or even human lives.
- Naval presence in the underwater domain; this mission is carried out mainly by submarines; it is enough for the enemy to know that the submarine is not in the port.

This force using operations can be achieved only by modern equipment such as sonars, surface and underwater drones or modern platforms such as Anti-Surface Warfare – ASW ships, submarines, torpedoes etc.

Examples of modern equipment that the Navy should consider to acquire can be: hydrographic maritime drones that can carry multiple sensors for underwater research and surveillance, mine warfare systems with the ability to detect, classify, localize, identify and neutralize drifting mines, midget submarines that can infiltrate into the enemy area of interest and collect data, medium size diesel-electric submarines for intel ops and attack potential enemies, and (semi) fixed seabed surveillance sensors.

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

As the significance of the seabed grows, there is a question about its role within the multi-domain environment. Although the seabed is not a distinct compartment or domain on its own, it does present a novel arena for potential conflict, necessitating vigilant monitoring and specialized doctrine. To effectively addresses the seabed warfare, it is imperative to identify both present and future threats to our national interests and the operational freedom of our armed forces. Specifically, the Romanian Navy and the affiliated intelligence directorates will play pivotal roles in detecting and identifying potentially hostile activities, comprehending the intentions of our adversaries, and attributing responsibility for such actions.

CONCLUSIONS

Incorporating the *seabed warfare* subject into the broader naval forces' doctrine goes beyond just recognizing and describing the operations that were outlined earlier. It necessitates crafting a distinct body of doctrine, delineating the framework, principles, and instruments essential for naval operations. This doctrine must be adapted to ongoing technological advancements, addressing critical areas like submarine communications, energy exploitation, underwater vehicle utilization, and so on. By comparative analysis, we have identified the different approaches to seabed doctrine. Most of them are concentrated around critical infrastructure protection and implementing underwater surveillance systems.

Acknowledging the experience of other states and the concern of some companies specialized in the submarine industry, and not only, regarding the importance of the underwater field, the Romanian Navy should consider introducing the concept of *seabed warfare* into its doctrine.

Acknowledging the experience of other states and the concern of some companies specialized in the submarine industry, and not only, regarding the importance of the underwater field, the Romanian Navy should consider introducing the concept of seabed warfare into its doctrine.

The three main functions presented:

- gain seabed expertise;
- conduct seabed surveillance;
- execute seabed operations,

are just some of the directives that must be adopted by the Navy in the future.

Technological advances in unmanned underwater vehicles and especially recent breakthroughs in autonomous underwater vehicles have helped to keep the seabed safe. On the other hand, technological developments have reopened the race to gain a degree of control of the seabed, making underwater critical infrastructure such as oil and gas platforms, telecommunications cables, and oil and gas pipelines more vulnerable to disruption, sabotage, linear or hybrid military action.

The Romanian Navy and other civil and military institutional actors must support the implementation of maritime security management

measures to cover the security of the seabed through active and passive measures. The military capabilities will be able to create the appropriate security framework for the safe exploitation of the underwater infrastructure, and the directly interested companies will be able to offer effective physical protection, complementary to general security.

BIBLIOGRAPHY:

1. Brooke, L. (May 2023). *Seabed Warfare Protecting the UKs Undersea Infrastructure*. London: UK Parliament, House of Common Library, https://commonslibrary.parliament.uk/seabed-warfare-protecting-the-uks-undersea-infrastructure, retrieved on 10.05.2024.
2. Calcagno, E., Marrone, A. (2023). *The Underwater Environment and Europe's Defence and Security.* Italy: Instituto Affari Internazionali.
3. Carr, C.J. et al. (June 2018). *Seabed Warfare and the XLUUV*. Monterey, Naval Postgraduate School.
4. Lade, C. (October 2022). *Saab sales manager and a former UK Royal Navy mine clearance diver*. Euronaval conference. Paris, https://defence.nridigital.com/global_defence_technology_dec22/seabed_warfare_is_a_real_and_present_threat, retrieved on 10.05.2024.
5. Metrick, H., Weinberger, S. (2016). *Undersea Warfare in Northern Europe*. Washington: Center for Strategic and International Studies.
6. Salerno-Garthwaite, A. (20 December 2022). *Seabed warfare is a 'real and present threat'Seabed warfare has moved on from hydrography and mine clearance as the sea floor infrastructure has exploded in scale*, https://www.naval-technology.com/features/seabed-warfare-is-a-real-and-present-threat/?cf-view, retrieved on 21.06.2024.
7. *Seabed Warfare Strategy* (2012). Report by the working group. France: Ministère des Armées, p. 38, https://www.defense.gouv.fr/en, retrieved on 18.06.2024.
8. Scipanov, L.V. (2020). *Possible solutions for the implementation of a strategy. The place of maritime strategy*. Gândirea militară românească, Statul Major al Apărării. București: Editura Centrului Tehnic-Editorial al Armatei, pp. 68-87. ISSN Print: 1454-0460 ISSN, Online: 1842-8231.
9. Scipanov, L.V., Nistor, F. (2019). *The timeliness of an underwater sensor system*. In Scientific Bulletin "Mircea cel Bătrân" Naval Academy, no. 2 (22), Constanța.
10. Scipanov. L.V., Sava, M. (2024). *Doctrinal approach to gain the seabed control – the case of Black Sea security.* In *Strategic Impact*, no. 2 (90), Bucharest.

11. https://defence.nridigital.com/global_defence_technology_dec22/seabed_warfare_is_a_real_and_present_threat, retrieved on 18.06.2024.
12. https://www.kongsberg.com/who-we-are/, retrieved on 10.06.2024.
13. https://www.kongsberg.com/maritime/about-us/news-and-media/blog-stories/seabed-warfare/, retrieved on 10.06.2024.
14. https://www.naval-technology.com/features/seabed-warfare-is-a-real-and-present-threat/?cf-view, retrieved on 21.06.2024.
15. https://www.saab.com/, retrieved on 10.05.2024.
16. https://www.saab.com/markets/norway/editorial-articles/seabed-warfare.
17. https://www.sercel.com/en, retrieved on 29.05.2024.
18. https://www.sercel.com/en/market/defense/submarine-warfare, retrieved on 29.06.2024.

ROMANIAN MILITARY THINKING

THE ROLE OF HEAVY ARMOUR IN MODERN WARFARE

Lieutenant Colonel Senior Instructor Claudiu Valer NISTORESCU, PhD

Command and Staff Faculty,
"Carol I" National Defence University, Bucharest

10.55535/RMT.2024.3.3

The end of the Cold War called an at least temporary halt to the idea of a conventional armed confrontation between two or more states with relatively equal capabilities. The need to manage unconventional and asymmetrical conflicts has led to a recalibration of military capabilities to respond effectively to new challenges. Western militaries have thus focused their efforts on achieving flexible and versatile capabilities. This new reality has naturally led to the constant neglect of heavy armoured forces. It is due to their relatively low utility in stability operations. However, recent conflicts, such as those in Nagorno-Karabakh and Ukraine, are bringing the need and desirability of using heavy armour in ground operations back to the forefront. Against this background, and with the unprecedented development of multi-spectral sensors, long-range, high-precision weapons and various unmanned platforms, the question arises as to whether heavy armoured capabilities still have a place in today's conflicts. The meticulous analysis of the current military phenomenon, in particular the Russian-Ukrainian conflict, has made it possible to obtain relevant results regarding the future and the possibilities for their development. The results are valuable in view of the initiatives taken by the Romanian Armed Forces to strengthen the armoured capabilities, in particular the steps taken to acquire new tanks, infantry fighting machines and self-propelled artillery.

Keywords: contemporary battlefield; heavy armoured formations; mobility; protection; firepower;

INTRODUCTION

NATO doctrine for land operations identifies three main types of tactical forces: *heavy forces*, *medium forces* and *light forces* (Allied Joint Publication, AJP-3.2 2022, B-1). While this categorisation of forces is not strict and mandatory for member states, it recognises that there are differences in the inclusion of forces in a particular category. Heavy forces are highly versatile, but their main role is to act in specific armed combat operations, carrying out a series of violent actions to defeat the enemy (Reynolds, 2023, p. 11). The description and assessment of the effects produced by these types of forces are based on the following parameters: *protection*, *firepower* and *mobility (figure 1)*. The way in which these three characteristics are balanced provides military commanders with options on how to conduct operations as well as warnings on the limitations, vulnerabilities and training needs of these forces.

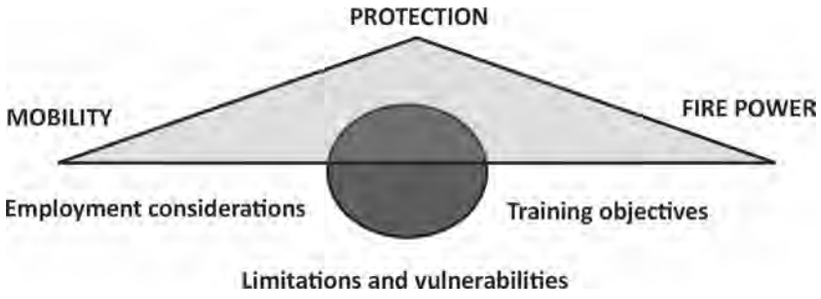


Figure 1: Determinants of heavy armoured forces (author's design)

Heavy forces include, in particular, tactical formations equipped with tanks, but also infantry forces operating on board heavily armoured infantry fighting machines and armoured combat search elements. As a general rule, the configuration of heavy armoured tactical formations aims to achieve a mix between tanks and armoured infantry units, the proportion depending on requirements and available capabilities. The main characteristics of this type of force are high firepower, extensive protection against enemy firepower,

Heavy forces include, in particular, tactical formations equipped with tanks, but also infantry forces operating on board heavily armoured infantry fighting machines and armoured combat search elements.

and high tactical mobility. These forces have a high degree of flexibility and shock capability, and their physical presence demoralises the enemy. However, despite these advantages, heavy armoured forces also have a number of limitations, such as reduced operational-strategic mobility, the ability to operate autonomously in restricted environments, special maintenance and supply requirements, and limited numbers of personnel who can operate as land forces. Reducing existing vulnerabilities means achieving a mix of heavy, medium and light forces operating in restricted terrain and training with these forces. With these considerations in mind, heavy armoured forces have generally been engaged in major offensive operations aimed at breaking through the enemy's defences, penetrating deep into the enemy's defences, then exploiting their success and pursuing them. Over the years, they have also proven their effectiveness in defensive operations, particularly in executing counterattacks or blocking the enemy.

The usefulness of armoured capabilities, particularly tank formations, is currently being debated by the scientific community. Their raison d'être is being questioned in the context of a battlefield contested on all fronts, where multispectral sensors and precision weapons severely limit manoeuvrability.

The usefulness of armoured capabilities, particularly tank formations, is currently being debated by the scientific community (Buzzard, 2023). Their raison d'être is being questioned in the context of a battlefield contested on all fronts, where multispectral sensors and precision weapons severely limit manoeuvrability (Johnson, 2022). The question of whether it is still cost-effective to develop an armoured platform amounting to about $5-6 million when it can be destroyed by an anti-tank missile that is up to twenty times less expensive makes therefore sense. In this context, both military experts and defence industry developers are assessing the performance of tanks and armoured vehicles in the heavy category. These assessments are aimed at reducing their vulnerability to anti-tank systems, in particular guided missiles, high-precision artillery rounds and air-launched attack vectors.

From the perspective of the aforementioned problematisation, the primary objective is to ascertain the role that heavy armour plays and will continue to play in contemporary conventional conflicts. In order to achieve this objective, we have conducted qualitative research, employing a longitudinal methodology to explore how heavy armour is used in operations. This approach has enabled us to identify critical situations in which these capabilities can generate a tactical advantage.

Additionally, the interpretative analysis of the contemporary military phenomenon has allowed us to identify threats and vulnerabilities to tank formations, as well as solutions for their reduction, including viable alternatives. In order to direct the research process, we have established the following primary research question:

- *In the future, will heavy forces be a key capability in warfare and, if so, what role will they play?*

This is corroborated by a series of subsequent inquiries, the responses to which are instrumental in achieving the research objective:

- *What are the principal threats to heavy armoured forces in the contemporary battlefield?*
- *What measures can be taken to mitigate the impact of threats to heavy armoured forces?*
- *What are the advantages of heavy armoured formations and how can they be effectively utilised?*

Recent assessments of the Russian-Ukrainian conflict have revealed that the two opponents employ their heavy armoured units in disparate situations, striving to identify solutions that enhance the efficacy of their actions.

Recent assessments of the Russian-Ukrainian conflict have revealed that the two opponents employ their heavy armoured units in disparate situations, striving to identify solutions that enhance the efficacy of their actions (Biddle, 2022). From this starting point, we are interested in examining how their doctrine, organisation and composition need to be recalibrated in order to meet the new requirements of the battlefield. The subject is a benchmark of interest in the context of the significant efforts being made by the allied states, including Romania, to strengthen existing military capabilities, including the creation of new capabilities, such as heavy armoured formations.

A HISTORICAL ANALYSIS OF THE EVOLUTION OF HEAVY ARMOUR

The tank, like the aeroplane, had a relatively limited initial deployment on the battlefield in the First World War, with these new capabilities being used intermittently and without a discernible impact on the overall operational landscape. The tank, initially a cumbersome platform, was designed to create corridors through the networks of non-explosive obstacles typical of that period *"trench warfare"*. Despite the significant impact it had on enemy morale, it was nevertheless relatively easy to counter, and the relatively small number of tanks available meant that they were only able to support

infantry in their assaults. However, both the tank and the aeroplane underwent steady development throughout the interwar period, thereby confirming their effectiveness during the Second World War. The German armed forces integrated the manoeuvring operations of armoured divisions with dive-bomber actions, marking the inaugural instance of such a combination in history. It established the foundations for the concept of *air-to-ground* operations, and the *tank-airplane* pair became the essential benchmark in the execution of conventional combat operations in the aftermath of the Great War. Consequently, most states engaged in an arms race invested heavily in developing such capabilities. The efficacy of these weapons was once again evidenced during the 1967 Six-Day War between Israel and Egypt. IDF (*Israeli Defence Force*) tank divisions, following a series of pre-emptive and destructive air strikes, overpowered the Egyptian defences, occupying the Sinai Peninsula. (Bowen, 2017). Nevertheless, the invincibility of Israel's tank divisions and air force was subsequently tested during the 1973 Yom Kippur War. New technologies provided manual or semi-automated guidance for guided anti-tank missiles[1], thus creating the conditions for the defeat of Israeli armoured structures. At the same time, the integration of new mobile surface-to-air missiles systems[2] in the Egyptian ground forces nullified the qualitative advantage of the enemy air force. The failure of the Israeli forces to assess the potential impact of the new technologies and to implement the concept of *"combined arms"* contributed to their inability to effectively engage with the initial phase of the conflict (Chorev, 1996). However, the IDF was able to achieve a doctrinal adaptation that drastically reduced the effectiveness of Egyptian operations due to the flexible approach. The Israelis reconfigured their formations to meet the requirements of the *"combined arms"* concept, and they also reconsidered their tactics in order to effectively hit Egyptian anti-tank teams, thereby reducing their effectiveness. (Bensahel, 2020, p. 62).

Both the tank and the aeroplane underwent steady development throughout the interwar period, thereby confirming their effectiveness during the Second World War. The German armed forces integrated the manoeuvring operations of armoured divisions with dive-bomber actions, marking the inaugural instance of such a combination in history.

In light of the accelerated development of cutting-edge technologies typical of the second half of the 20th century, the arms-versus-arms competition has persisted. Major competing powers have analysed the impact of new technologies on the development of military organisation and introduced the concept of a *Revolution in Military Affairs/RMA* to mark the beginning of a period in which technological supremacy becomes a fundamental benchmark for success on the battlefield (Sloan, 2008, p. 8). In the context of armoured formations, which constituted the dominant capabilities during the Cold War, specialists have concentrated their efforts on enhancing their armour plating, as well as increasing their mobility and firepower. New protective systems are being developed, such as *explosive-reactive armour/ERA*, which serves to diminish the effectiveness of anti-tank missiles. The countermeasure has been intrinsic and comprised the development of missiles with dual tandem warheads, which permit penetration of the ERA. Furthermore, attack helicopters, equipped with such missiles, facilitate the striking of armour from considerably greater distances than ground-based platforms. However, technological advancement has once again ensured the continued viability of armoured capabilities. US Army military doctrine, developed in the late 1980s and known as *AirLand Battle*, identifies technological superiority as the primary factor in compensating for a quantitative inferiority (Douglas, 1998, p. 11). The doctrine in question was predicated on the utilisation of sophisticated technologies, including advanced communications, satellite positioning and navigation systems, stealth technology, laser, radio wave, thermal spectrum and GPS guidance systems. Despite its ostensible purpose of providing a solution to counter potential Soviet aggression in Europe, the AirLand Battle doctrine was successfully tested in the 1991 Gulf War. The integration of new capabilities at the joint level facilitated new capabilities synergising at the battlefield level, while simultaneously reducing the vulnerability of heavy armoured formations. Consequently, the deployment of novel weaponry, including the M1 Abrams tank, the M2 Bradley infantry fighting vehicle, and the MIM-104 Patriot air defence system, supported by AH-64 Apache and UH-60 Black Hawk helicopters, collectively constituted *the big five* concept, being the prerequisites for a swift victory in Operation Desert Storm. (Ortiz, 2021).

ROMANIAN MILITARY THINKING

Major competing powers have analysed the impact of new technologies on the development of military organisation and introduced the concept of a Revolution in Military Affairs/ RMA to mark the beginning of a period in which technological supremacy becomes a fundamental benchmark for success on the battlefield.

[1] Soviet Malyutka (NATO code AT-3 Sagger) Anti-Tank Guided Missile/ATGM of Soviet origin (A.N.).

[2] Soviet 2K12 *"KUB"* (SA-6 *"Gainful"*) mobile surface-to-air missile system of Soviet origin (A.N.).

THREATS TO HEAVY ARMOURED FORMATIONS

In this section, we will return to the role of heavy armoured formations in the context of the modern battlefield. We will attempt to ascertain the extent to which new threats have called the utility of such formation into question. The analysis of the conflicts in Nagorno-Karabakh, Ukraine and the Gaza Strip demonstrates the continued maintenance of heavy armoured capabilities and the tendency of armies to employ them in both offensive and defensive operations. Furthermore, these conflicts illustrate the emergence of novel threats that challenge the efficacy of heavy armoured capabilities on the battlefield, as well as the maintenance and adaptation of existing ones. The threat spectrum encompasses a range of sophisticated technologies, including state-of-the-art guided anti-tank missiles, precision munitions, ISR and UAS capabilities with strike capabilities, loitering munitions and minefields.

Top-attack or flying top-attack functions permit the targeting of armour from a high position, focusing on the vulnerable upper portion of the armoured platform.

❖ *The guided anti-tank missiles*

The advent of new technologies has enabled guided anti-tank missiles to develop capabilities that permit strikes on tanks from distances exceeding 4,000 metres and in innovative ways that exploit the vulnerabilities of armour. *Top-attack* or *flying top-attack* functions permit the targeting of armour from a high position, focusing on the vulnerable upper portion of the armoured platform. The dual tandem searchlights of the latest-generation missiles facilitate the neutralisation of additional protective measures, such as the ERA or the renowned Russian *"cages"*. The missile's *fire* and *forget* function enables its launch without the direct involvement of the launch team, who can then be extracted immediately after launch, rendering countermeasures against them ineffective.

The missile's fire and forget function enables its launch without the direct involvement of the launch team.

❖ *High precision ammunition*

Smart munitions, with their high accuracy and extended range, make it possible to engage enemy armoured vehicles outside the contact zone. The lethality of in-theatre attacks is directly proportional to the accuracy of the ammunition and the weapon system. To increase accuracy, two essential conditions must be met: *the process of identifying, monitoring and engaging a target through the utilisation of various intelligence, surveillance and reconnaissance*

(ISR) systems, coupled with *the deployment of in-flight munitions guidance technologies, employed to guarantee that the intended target is successfully engaged.* The advent of high technology in recent decades has facilitated the development of artillery ammunition with an extended range of up to 50 km and high accuracy, achieved through the integration of GPS-INS (inertial navigation system) technology. A notable example of this category of ammunition is the US Army's Excalibur M982 artillery projectile, which is also being developed in various variants for other NATO militaries. The advantages of this type of ammunition are considerable, as it can be used with conventional weapon systems (155 mm calibre howitzers), allowing them to be guided by GPS. The Guided Multiple Launch Rocket System (GMLRS) is also considered a game changer, with its capacity to strike targets with precision and at ranges that are competitive with other systems. It is notable for its ability to outperform similar systems that are more massive and less accurate. (RAND Corporation 2015, p. 15). These weapon systems are designed for deployment at the division and corps levels. They offer high mobility and high firepower, and are available in both tracked and wheeled configurations. The modern variants integrate GPS-INS munitions technology, which enables the munitions to be guided to the target location, with a circular probable error/CEP of 5-10 meters for the US Army GMLRS systems. (Ib., p. 32). Both smart munitions artillery systems and GMLRS provides a distinct advantage upon the defending force in the context of a battle against armoured vehicles. It is due to their capacity to facilitate early engagement of artillery in the event of successful detection and the temporary blocking of enemy columns.

Both smart munitions artillery systems and GMLRS provides a distinct advantage upon the defending force in the context of a battle against armoured vehicles. It is due to their capacity to facilitate early engagement of artillery in the event of successful detection and the temporary blocking of enemy columns.

❖ *ISR Capabilities*

The diversity of multispectral sensors presents a significant challenge to the armoured formation's concealment. Ensuring the security of these operations was challenging due to the extensive multispectral footprint. Furthermore, ISR capabilities provide not only information about the presence of enemy forces in specific areas but also detailed information about their nature, value, capabilities, and even intentions. A surveillance system calibrated to cover all operational domains while connected to strike systems through a sensor-to-shooter relationship can streamline the target engagement and destruction cycle.

❖ *Unmanned Aerial Systems/UAS with strike capabilities*

These systems, whether intended for reconnaissance and/or attack, can play an important role in the battle against armoured vehicles. They can do so by gaining intelligence on enemy operations and correcting the fire of their own forces, and by striking at the enemy's armoured capabilities. Their deployment has been successfully demonstrated in low-intensity conflicts over the past two decades. The effectiveness of these systems was evidenced in counter-insurgency operations in Iraq and Afghanistan, as well as in large-scale operations against ISIS in Mosul and Raqqa. Unmanned Aerial Vehicles (UAVs) gained notoriety in 2020, during the Nagorno-Karabakh armed conflict, for their effectiveness in combat operations. The successful deployment of the Turkish-built Bayraktar TB2 attack drones by the Azerbaijani army has prompted an academic debate as to whether these systems are indeed a *"tool"* that will significantly shape the way combat operations are conducted in the future. (Hecht, 2022). In an analysis of the Nagorno-Karabakh conflict, Israeli expert Uzi Rubin, the founder of *Israel's Long-Range Missile Defence Program*, emphasized the crucial role played by the Bayraktar TB 2 systems: *"Azerbaijani systems were instrumental in the destruction of Armenian air defence capabilities and the subsequent decimation of manoeuvre forces, including tanks, artillery and logistical support vehicles. These violent attacks forced Armenia to accept a humiliating peace deal imposed by Russia".* (Rubin, 2020).

The successful deployment of the Turkish-built Bayraktar TB2 attack drones by the Azerbaijani army has prompted an academic debate as to whether these systems are indeed a "tool" that will significantly shape the way combat operations are conducted in the future.

The versatile capabilities of this type of UAS have also been successfully demonstrated in Ukraine, particularly during the initial phase of the conflict. The inconsistent anti-aircraft defences of Russian forces engaged in offensive operations permitted the infiltration of Ukrainian Bayraktar TB 2 systems and the striking of Russian armoured vehicles. Despite the prolongation of the Russian-Ukrainian conflict, which has resulted in a continuous adaptation of both combatants to counter UAS, it is anticipated that these capabilities will become a significant shaping vector on the battlefield in the future, including in the battle against armour.

❖ *Loitering ammunition*

While loitering munitions are capable of generating effects at all levels of operations, they play a predominantly shaping role in armour combat. Their relatively low strike vector mass and platform targeting

limitations result in a notable reduction in their overall effectiveness (Pettyjohn, 2024). Consequently, the impact of these types of munitions is relatively limited in terms of impeding the manoeuvring capabilities of armoured units. However, they can cause significant destruction and demoralisation, particularly for isolated manoeuvre elements engaged in tactical defensive operations. Despite the view of military experts that their role in combat against armoured vehicles is not decisive, they can nevertheless generate a number of effects with the objective of harassing the enemy, temporarily blocking their movement, disorganising their operations and affecting the cohesion of their actions. They can be effective against small armoured elements, whether stationary or moving, which do not benefit from adequate anti-aircraft defences. Second echelon, armoured elements or armoured reserves deployed in rear areas can be successfully hit by tactical systems, even at night. Such munitions were employed by the Azerbaijani army in the Nagorno-Karabakh conflict and are also being utilised in combat operations in Ukraine. It is inevitable that they will continue to evolve, becoming increasingly versatile and generating more diverse and profound effects on the configuration and dynamics of the battlespace.

ROMANIAN MILITARY THINKING

❖ *The minefields*

Minefields represent the optimal solution for creating an obstacle in flat terrain, with effectiveness contingent upon depth, density, and fire cover possibilities. The Ukrainian counteroffensive in the summer of 2023 exemplifies the efficacy of these defensive tactics and their capacity to block armoured vehicles. The increased depth and density of the minefields constructed by the Russians exemplify the effectiveness of defensive lines built in accordance with tactical adaptations derived from experience gained in the initial year of the conflict (Reynolds, p. 15).

Minefields represent the optimal solution for creating an obstacle in flat terrain, with effectiveness contingent upon depth, density, and fire cover possibilities. The Ukrainian counteroffensive in the summer of 2023 exemplifies the efficacy of these defensive tactics and their capacity to block armoured vehicles.

SOLUTIONS TO REDUCE THE THREAT'S IMPACT

The initial phase of the conflict in Ukraine revealed the vulnerabilities of Russian armoured units, which suffered significant losses, particularly on the Belarus-Kyiv and Belgorod-Kharkiv offensive fronts. However, the failure of the Russian Federation's tank formations was more likely attributable to inadequate planning and integration

of offensive operations at the joint level throughout the course of the operation (Lee, 2022). The commanders of the armoured units failed to anticipate a staggered and layered defence of the Ukrainians. Consequently, they advanced independently in several offensive directions, their actions being inadequately coordinated by the higher echelon. Furthermore, the accelerated pace of the offensive resulted in the lack of synchronisation between manoeuvre forces and combat and logistical support forces. The inadequate artillery, air defence and electronic warfare capabilities, which were already insufficient, were unable to maintain the same pace of the offensive, and the same difficulties were encountered in the logistics. The lack of integration at the joint level had significant ramifications for the Russian battlegroups/BTGs: manoeuvre forces lacking combat support were subjected to Ukrainian artillery and drone attacks; the scarcity of fuel and spare parts compelled crews to abandon their tanks and combat vehicles; support elements were persistently targeted by Ukrainian light infantry infiltrating the area. A review of data from the *Oryx blog* suggests that, as of early April 2022, over 30% of the tanks lost by the Russians were due to either failure or abandonment. (Janovsky, 2022). It provides further evidence in support of the hypothesis that the offensive operation was poorly planned and executed. The inadequate composition of the Russian BTGs, in particular the lack of infantry elements, also created dysfunctions that manifested in the inability to effectively execute tactical cover, surveillance and close protection missions (Lee, ib.).

A review of data from the Oryx blog suggests that, as of early April 2022, over 30% of the tanks lost by the Russians were due to either failure or abandonment. It provides further evidence in support of the hypothesis that the offensive operation was poorly planned and executed.

In the context of the Nagorno-Karabakh conflict, Oryx reports that Armenia lost 255 tanks, 146 of which were destroyed by Turkish Bayraktar TB2 systems. The remaining tanks were neutralised by artillery and anti-tank missiles, following the exploitation of intelligence gathered by drones (Janovsky, 2020). While these systems were responsible for over 85% of the Armenian heavy armoured losses, their poor performance was not the sole cause. Western analyses indicate that Bayraktar TB2 platforms were only engaged decisively after the destruction of the Armenian forces' anti-aircraft defences, with air supremacy being a crucial factor (Jones, 2022).

In light of the aforementioned considerations, it can be concluded that heavy armour will play a role in future conventional armed confrontations. Gaining a tactical advantage through the use of heavy

armour formations depends, in particular, on the ability to use them intelligently, reducing their vulnerabilities. The following section presents several potential solutions that can increase the effectiveness of heavy armour formations in combat operations.

The effective exploitation of heavy armour requires a robust foundation in the form of a well-defined manoeuvre approach to operations. This approach must be integrated at the unit level to ensure its successful implementation. In large-scale offensive operations, tanks must be adequately supported by heavy and medium infantry units. Artillery support and air defence capabilities can be achieved through the integration of self-propelled platforms that offer comparable levels of protection and mobility. It is imperative that robust search and combat engineering capabilities should be in place to guarantee the mobility of the main forces, threat warning and battlefield shaping. When operating in restricted terrain (mountainous environment, urban environment), dismounted infantry elements provide invaluable support to heavy armour operations, as do anti-ambush teams or air defence teams equipped with Man-Portable Air-Defence Systems/MANPAD. The incorporation of unmanned aerial systems/UAS elements into heavy armoured units offers the potential for early warning and fire coordination capabilities, which could be employed to neutralise threats. Finally, electronic warfare/EW systems may be useful for neutralising threats whose effects depend on the possibility of exploiting the electromagnetic spectrum, including drones and guided anti-tank missiles.

In order to neutralise or reduce the level of threat posed by anti-tank missiles, both *hard kill* and *soft kill* measures are integrated into blast. *Hard kill* measures entail the integration of an active protection system/APS within the platform. This system employs a short-range radar to detect and track the threat, utilising electron-optical sensors to identify the threat in the vicinity of the target, and employing explosive measures (projectile or charge) to neutralise the target, detonating the strike before impact. The objective of *soft kill* measures is to disrupt the guidance channel of anti-tank or smart munitions, either at the point of initial launch or during the flight to the target. It is achieved by jamming the radio link, short-circuiting the electro-optical link or the communication unit.

In order to neutralise or reduce the level of threat posed by anti-tank missiles, both hard kill and soft kill measures are integrated into blast. Hard kill measures entail the integration of an active protection system/APS within the platform.

To counter extended-range, high-precision strike capabilities, the first step is to intensify efforts to neutralise enemy ISR elements that provide information on the location and armoured forces' activities. It will be achieved by concentrating the efforts of air defence and EW capabilities. Force camouflage is also a solution, as are false works (including mock-ups) and deception operations to increase protection from enemy attack. However, these operations, under the umbrella of C2D2 (cover and concealment, decoy and deception), must be consistent and viable in all operational areas where their effects can be intercepted and assessed (Toroi, 2024). For instance, scale models must be credible in terms of their visual, thermal and electromagnetic representation. Furthermore, the deployment of a significant military unit in a particular area must be reflected in media activities and on specific social networks.

In anticipation of the Ukrainian counteroffensive in the summer of 2023, Russian forces had several months to establish an elaborate fortification system in the Zaporizhzhya region. Similarly to the Battle of Kursk 80 years ago, the Russians were able to mitigate the impact of the enemy's offensive actions. In both instances, the culmination of the attack occurred weeks later.

The overcoming of minefields and the achievement of a breakthrough necessitate the coordinated action of all available capabilities at the operational level. Consequently, this challenging task commences with aerial reconnaissance of the penetration area, the neutralisation of the enemy's anti-aircraft defences and the striking of the enemy's artillery and missile systems. Thereafter, a heavy armoured force, supported by engineer elements, creates the requisite corridors through the minefields and ensures the safety of these corridors, thus facilitating the introduction of the main forces into the fight. The success of this action is contingent upon the swift execution of operations and the effective collaboration of supporting arms with manoeuvre forces. The implementation of concealment is of paramount importance for enhancing the probability of success. Conversely, it is imperative to underscore that constraining the time available to the defending force for the construction of defensive lines increases the chances of success for the offensive. In anticipation of the Ukrainian counteroffensive in the summer of 2023, Russian forces had several months to establish an elaborate fortification system in the Zaporizhzhya region. Similarly to the Battle of Kursk 80 years ago, the Russians were able to mitigate the impact of the enemy's offensive actions. In both instances, the culmination of the attack occurred weeks later.

THE ADVANTAGES OF MAINTAINING AND DEVELOPING HEAVY ARMOURED FORMATIONS

The specific design of heavy armour provides a high degree of stability for ground forces. Concurrently, their high lethality and capacity to instil shock serve as a deterrent to potential aggressors, exemplifying a willingness to utilize lethal measures when necessary. Consequently, they become a symbol of the state's military strength. However, the maintenance and advancement of these capabilities by potential adversaries necessitates a counterbalancing response, which can be achieved through the development of robust anti-tank capabilities and the creation of analogous armoured capabilities.

This type of force, comprising tanks, mechanised infantry, combat reconnaissance and armoured engineer elements, represents an effective solution for the opening of a theatre of operations. Furthermore, in the context of the rapid development of offensive operations, these forces can be formed into forward detachments whose missions are to penetrate the enemy's equipment, intercept enemy communication routes, and capture and hold important objectives. They are the only viable solution for breaching enemy minefields. Furthermore, they permit the operation to evolve in a gradual and controlled manner, enhancing preliminary strikes, disrupting adversarial defences, and rapidly capitalizing on emerging opportunities. Finally, with the support of combat helicopters, self-propelled artillery, mechanized infantry, and engineer elements, they are capable of successfully conduct pursuit operations.

The deployment of heavy armoured forces serves to reinforce the defensive position. Their objective is to rapidly address any gaps created by enemy action and to launch counter-attacks with the aim of restoring the original defensive perimeter and recapturing lost territory. Heavy armoured forces are the primary means of impeding the advancement of enemy tanks.

The deployment of heavy armoured forces serves to reinforce the defensive position. Their objective is to rapidly address any gaps created by enemy action and to launch counter-attacks with the aim of restoring the original defensive perimeter and recapturing lost territory. Heavy armoured forces are the primary means of impeding the advancement of enemy tanks. They also play a crucial role in delaying operations, as their high mobility and protection enable the successful execution of these missions. Heavy armoured forces assume a pivotal role in mobile defence operations, as they are well-suited for executing decisive counter-attacks aimed at encircling and destroying penetrating enemy forces.

Despite their vulnerability in urban environments when operating without infantry support, these forces are highly effective when the enemy has a robust defence with fortified strong points. The combined action of tanks, tank support infantry and dismounted infantry significantly enhances the probability of armoured survival in the urban combat environment (Allied Tactical Publication, 2022, p. 31). Infantry provides close protection, while tanks destroy hardened fighting positions and machine gun nests. The deployment of heavy armour in peace-enforcement operations in environments dominated by insurgent action is also a viable option. The high ballistic protection and mine resistance inherent to this type of armour affords them a distinct advantage in this respect.

The combined action of tanks, tank support infantry and dismounted infantry significantly enhances the probability of armoured survival in the urban combat environment. Infantry provides close protection, while tanks destroy hardened fighting positions and machine gun nests. The deployment of heavy armour in peace-enforcement operations in environments dominated by insurgent action is also a viable option.

Over time, solutions have been sought to replace and/or substitute these capabilities. Medium forces demonstrate relatively the same lethality and tactical mobility while being more versatile in terms of transportation and employment in restricted environments. However, their lower protection compared to that of heavy forces would result in a significantly higher number of human casualties, which could outweigh the advantages of their use in missions that require the capabilities of heavy armoured forces. The deployment of light forces, with their capacity to form agile anti-tank units, can have a decisive impact in armoured combat, although their role is primarily that of a shaping force. The synchronised application of tactics and techniques to counter anti-tank ambushes can significantly reduce their effectiveness. Consequently, the strategic use of heavy armour can provide commanders, particularly in large-scale conventional operations, with clear advantage.

CONCLUSIONS

This approach offers a solution to the research questions that serve as the foundation for the study's objectives. It seems probable that heavy armour will continue to play a significant role on the modern battlefield. The advantages offered by these robust capabilities as well as the existing trends in platform modernisation, adaptation and doctrines empirically validate this assumption. Furthermore, efforts by an increasing number of states to strengthen these capabilities reinforce this idea. However, in order to maximise their chances of success in a major armed conflict, a number of considerations need to be taken into account by both political-military decision-makers and military commanders.

The enhancement of strategic mobility for heavy armour represents a critical concern in the development and sustainment of these types of military forces. The relatively low speed of movement, high platform wear and tear, and infrastructure constraints imposed by the use of tanks significantly restrict their operational capabilities. Consequently, the transportation of these capabilities along various communication routes must be calibrated to ensure the protection of personnel during transit, adhere to time constraints, and facilitate rapid operational deployment. While air transportation is the most expedient mode of travel, its availability is constrained by the aircraft capacity. Although maritime transportation is an efficient mode of transport, it is important to consider the necessity for ports and port infrastructure, as well as the availability of post-landing transportation options. Of the land transportation options, rail is probably the most efficient, although it is important to consider traffic fluidity and protection during movement. A reduction in the mass of armour, particularly that of heavy tanks, is an important factor in operational-strategic mobility. However, it should not result in a detrimental compromise in terms of protection and firepower. Consequently, the tank and other heavy armoured vehicles must retain their main assets in terms of *design* and performance, namely the ability to destroy other tanks and maintain *momentum* in the offensive operation.

The relatively low speed of movement, high platform wear and tear, and infrastructure constraints imposed by the use of tanks significantly restrict their operational capabilities. Consequently, the transportation of these capabilities along various communication routes must be calibrated to ensure the protection of personnel during transit, adhere to time constraints, and facilitate rapid operational deployment.

From an operational standpoint, it is crucial to adopt a joint perspective at the tactical level when approaching land operations, as well as to integrate tactical land operations at the joint operation level. This approach can enhance the survivability of heavy armoured units and facilitate the exploitation of their potential. It is therefore essential that these capabilities retain their status as the principal means of conducting major combat operations. The ability to maintain a high level of force dispersion while also rapidly concentrating to execute missions is crucial for the survival of armoured forces on a battlefield. The integration of sophisticated technologies designed to identify and neutralise threats enhances the probability of success. Furthermore, the advancement of active and passive *hard* and *soft kill* protection

systems represents a significant step towards aligning heavy armour with the demands of emerging technologies.

It seems inevitable that the tank-anti-tank competition will persist. The tactical adaptation will facilitate the expeditious resolution of particular issues encountered on the battlefield, whereas institutional adaptation will facilitate the formulation of strategies for the advancement of armoured capabilities and the development of doctrines that will underpin their employment. Nevertheless, as the Javelin and NLAW guided anti-tank missiles have not resulted in effects of greater magnitude than those achieved by the Sagger in the Yom Kippur War, there is no guarantee that future systems will definitively and irrevocably defeat heavy armoured forces. The essence of warfare is enduring, being characterised by violence. Heavy armoured capabilities represent weapons that, when deployed effectively, can inflict significant levels of destruction in order to achieve defined military goals. The research findings validate their continued relevance on the contemporary battlefield, as well as the capacity of the military organisation to adapt them to meet the demands of the evolving nature of warfare.

The essence of warfare is enduring, being characterised by violence. Heavy armoured capabilities represent weapons that, when deployed effectively, can inflict significant levels of destruction in order to achieve defined military goals.

BIBLIOGRAPHY:

1. Allied Joint Publication (2022). AJP-3.2. *Allied Joint Doctrine for Land Operations.* Edition B version 1. Belgium: Brussels. NATO Standardization Office (NSO).
2. Allied Tactical Publication (2022). ATP-3.2.1.3. *Conduct of Land Tactical Operations in Urban Environments.* Edition B Version 1. Belgium: Brussels. NATO Standardization Office (NSO).
3. Bensahel, N., Barno, D. (2020). *Adaptation under Fire – How Militaries Change in Wartime.* Oxford: Oxford University Press.
4. Biddle, S. (22 November 2022). *"Ukraine and the Future of Offensive Maneuver on 18.11.2023"*. *War on the Rocks*.
5. Bowen, J. (5 June 2017). *"1967 War: Six Days that Changed the Middle East". BBC News*.
6. Buzzard, C.A., MG, Feltey, T.M., BG, Nimmons, J.M., LTC, Schwartz, A.T., M, Dr. Cameron, R.S. (August 2023). *"The Tank Is Dead… Long Live the Tank"*. In *Military Review*, https://www.armyupress.army.mil/journals/military-review/online-exclusive/2023-ole/the-tank-is-dead/, retrieved on 21 May 2024.
7. Chorev, M. (1996). *Surprise Attack: The Case of The Yom-Kippur War.* Research Report. Washington D.C.: The Industrial College of the Armed Forces. National Defense University, retrieved on 20 January 2023.
8. Douglas, S. (1998). *Airland Battle Doctrine.* Alexandria. Virginia: Center for Naval Analyses/CNA.
9. Hecht, E. (2022). *"Drones in the Nagorno-Karabakh War: Analyzing the Data".* In *Military Strategy Magazine* 7, no. 4, pp. 31-37.
10. Janovsky, J., Stijn Mitzer, D., Oliemans, J. (27 September 2020). *The Fight for Nagorno-Karabakh: Documenting Losses on the Sides of Armenia and Azerbaijan.*
11. Janovsky, J. (2022). *"Attack on Europe: Documenting Russian Equipment Losses During the Russian Invasion of Ukraine".* Oryx.
12. Johnson, D.E. (8 April 2022). *"The Tank Is Dead: Long Live the Javelin, the Switchblade, the…?"*. *War on the Rocks*, https://warontherocks.com/2022/04/the-tank-is-dead-long-live-the-javelin-the-switchblade-the/, retrieved on 21 May 2024.
13. Lee, R. (6 September 2022). *"The Tank Is Not Obsolete, and Other Observations about the Future of Combat"*. *War on the Rocks*.
14. Ortiz, M. (27 January 2021). *"The 'Big Five' systems that helped win Desert Storm"*. *We Are the Mighty*.
15. Pettyjohn, S.L. (March 2024). *"Drones Are Transforming the Battlefield in Ukraine but in an Evolutionary Fashion"*. *War on the Rocks*.
16. RAND Corporation (2015). *Comparing U.S. Army Systems with Foreign Counterparts – Identifying Possible Capability Gaps and Insights from Other Armies.* Scientific Report. Santa Monica.
17. Reynolds, J., Watling, N. (2023). *Stormbreak: Fighting through Russian Defences in Ukraine's 2023 Offensive.* Special Research Report. London: Royal United Services Institute for Defence and Security Studies.
18. Reynolds, N. (2023). *Heavy Armoured Forces in Future Combined Arms Warfare.* London: Royal United Services Institute for Defence and Security Studies.
19. Rob, L., Kofman, M. (22 June 2022). *"Not Built for Purpose: The Russian Military's Ill-Fated Force Design"*. *War on the Rocks*.
20. Rubin, U. (2020). *"The Second Nagorno-Karabakh War: A Milestone in Military Affairs".* In *Mideast Security and Policy Studies* (The Begin-Sadat Center for Strategic Studies Bar Ilan University), no. 184: 5.
21. Seth, G.J., Harrington, J., Reid, C.K., Stohmeyer, M. (2022). *Combined Arms Warfare and Unmanned Aircraft Systems.* International Security Project. Center for Strategic&International Studies, Washington: Rowman&LittleField, 10.
22. Sloan, E. (2008). *Military Transformation and Modern Warfare: A Reference Handbook.* London: Praeger Security International.
23. Toroi, G.-I. (7 June 2024). *"Enhancing Operational Protection: A Step-By-Step Counter-Deception Guide".* In *Scientific Bulletin of the Nicolae Bălcescu Land Forces Academy*. Vol. 29, no. 1, pp. 179-188, https://doi.org/10.2478/bsaft-2024-0019.

THE CASE FOR ENHANCING THE ROLE OF DECEPTION IN ROMANIAN MILITARY DOCTRINE

Lieutenant Colonel George-Ion TOROI, PhD
"Carol I" National Defence University, Bucharest
10.55535/RMT.2024.3.4

The 80th anniversary of the largest amphibious operation in history, the D-Day landings in Normandy on 6 June 1944, also brings to mind a concept critical to the success of that military operation: deception. Creating and gaining operational advantage on the battlefield by manipulating the enemy's perception has always been a desideratum for any military force.

Although the art of deception received somewhat less attention in Western military doctrine at the beginning of this millennium, it has become increasingly important in recent years due to the heightened competition between the great powers, being considered critical to the success of current military operations.

In this context, the article aims to sensitise Romanian military decision-makers at all levels with respect to the operational necessity of deception, the need to perfect specific skills during the training process, as well as to the development of an appropriate doctrinal framework that will contribute to the consolidation of the Romanian Armed Forces' combat power.

Keywords: deception; cognitive domain; operating environment; technology; operational advantage;

ROMANIAN MILITARY THINKING

Motto:
"In wartime, truth is so precious that it should always be attended by a bodyguard of lies".
Winston Churchill

INTRODUCTION

Recently, it has been 80 years since the greatest amphibious military operation in history – *the Normandy landings of 6 June 1944* –, when the Allies succeeded in projecting a considerable military force ashore that ultimately contributed significantly to the defeat of Nazi Germany in the First World War. The remembrance of those moments, in addition to the courage and heroism of the soldiers who fought at the time, brings to the fore an extremely important aspect of the art of war, which contributed significantly to the success of the whole operation, namely the *art of deception*. Without the careful planning and execution of *Operation Bodyguard*, the Allied deception plan, the casualties suffered and even the success of the landings might have been in doubt. The role of deception was therefore crucial in ensuring favourable landing conditions for the Allied forces by manipulating the enemy's perception to the exact place and time of the landing.

Without the careful planning and execution of Operation Bodyguard, the Allied deception plan, the casualties suffered and even the success of the landings might have been in doubt. The role of deception was therefore crucial in ensuring favourable landing conditions for the Allied forces by manipulating the enemy's perception to the exact place and time of the landing.

A crucial element, also part of the deception operation, was to maintain a false perception of the direction of the main Allied operational effort even after the initial landings had taken place. It ensured that the Germans kept the bulk of their forces in places of no operational importance, thus supporting the rapid and secure build-up of Allied forces on the Normandy beaches.

It can therefore be seen that the purpose of misleading actions is to materialise operational opportunities leading to decisive advantages over the enemy. This was the case in *Operation Bodyguard*, where all the actions taken led to the success of the Normandy landings. The example is not unique, however, and history is littered with instances of military commanders exploiting human nature to deceive

their adversaries and create the conditions for operational success (Kennedy, 2022, p. 306).

However, while history has demonstrated the undeniable value of such actions, **the ability of Western militaries to plan and execute them has declined significantly in recent decades**. (Strategic Survey 2022. The Annual Assessment of Geopolitics, 2023, p. 40). I consider that the main reasons that have led to such a situation are the following:

- the unipolarity of the global system installed after the dissolution of the USSR;
- the nature of the counter-insurgency operations and the adversaries encountered in armed confrontations, without the need to find ingenious solutions in a technologically dominated battlefield;
- the misperception of deception ineffectiveness in a highly transparent operational environment.

"A return to great power competition against peer adversaries with advanced anti-access/area-denial (A2AD) capabilities will require a renewed focus on the employment of deception".

RESEARCH GAP

However, against the backdrop of the paradigm shift of armed conflicts towards large-scale combat operations, in the context of the evolution of society towards a multipolar society characterised by an intense level of competition (Joint Doctrine Note 1-19 Competition Continuum, 2019, p. 1; Mazarr J.S., 2018, p. 1; Mazarr J.B., 2022, pp. 111-113; MCDP 1-4 Competing, 2020, pp. 1-3) as well as of an arms race between East and West, the importance of finding solutions that provide operational advantages to one side becomes crucial. For example, it is recognised that *"a return to great power competition against peer adversaries with advanced anti-access/area-denial (A2AD) capabilities will **require a renewed focus on the employment of deception**"*. (Hays, 2020, p. 56).

If we also take into account **the human side of the conflict**, it becomes essential to achieve effects in the opponent's cognitive dimension, by influencing his understanding and will to fight. At the same time, although we are witnessing an extremely rapid development of technology, with implications in all branches of military science and art, I am aware that, in the short and medium term, decision-making

will continue to be based on the human factor. Therefore, exploiting the limitations of the human brain through the use of deceptive actions can make a significant contribution to the achievement of operational advantages in the tactical field, according to B.A. Friedman. (Friedman, 2017, p. 31).

Today we are also witnessing a profound transformation of society through **unprecedented technological development**. Things that not so long ago seemed to be the stuff of science fiction have become reality. The trend continues to accelerate. Identifying a legal framework to regulate the impact and use of these new technologies is extremely difficult at this stage. As one of the main pillars of any society, the military sector could not fail to be affected by these changes. Today, we are witnessing an almost total digitalisation of all branches of the military system, the implementation of artificial intelligence to facilitate the processing of the multitude of data in the information environment and thus support decision-making, the integration of robots to perform specific armed combat functions, and the development of radars and sensors for intelligence gathering. Within this framework, the **current operational environment** has become extremely complex and ambiguous (JCN1/17, 2017, p. 1; Future Leadership, 2020, pp. 1-2; TC 7-102, 2014, pp. 1-2), providing the right conditions for misleading.

ROMANIAN MILITARY THINKING

We are witnessing an almost total digitalisation of all branches of the military system, the implementation of artificial intelligence to facilitate the processing of the multitude of data in the information environment and thus support decision-making, the integration of robots to perform specific armed combat functions, and the development of radars and sensors for intelligence gathering.

However, there is a school of thought among some military theorists that deception is no longer possible due to the increased transparency of the battlefield brought about by the technological developments in the military field. However, the ongoing conflict in Ukraine shows that **this art is by no means obsolete**. More than ever, it has become critical to maintaining the operational capability of the armed forces or to achieving surprise and operational advantage on the battlefield. Its viability is also demonstrated by Australian General Mick Ryan's observation that *"the ability to observe more on the battlefield does not necessarily ensure a greater degree of insight into what is actually happening or what the enemy is thinking"*. (Ryan, 2024). In other words, being able to observe the battlefield is not enough to understand the operational situation.

The main research gap that generated this study is that the Romanian Armed Forces do not take sufficient measures, at both theoretical and practical levels, to include deception as a defining element of the Romanian operational art.

I see it as a paradox, as there is a growing awareness of the importance of this issue in contemporary military operations. The above conclusion is the result of an open-ended **questionnaire** that I conducted in 2023 in order to identify counter-deception solutions in the current operational environment. One of the secondary objectives of this questionnaire was to also find out *how officers in the Romanian Armed Forces perceive the concept of deception*. In this respect, of the 73 respondents who were asked to rate, on a scale of 1 to 10, their own degree of willingness to engage in deception in a potential military operation, the resulting average was extremely high, namely 8.54. I should mention that the selection of the personnel who participated in the questionnaire during the sampling process was made according to the following criteria: professional experience, which is shown in *table 1*, as well as their level of knowledge, selecting only officers enrolled in the Combined Arms Master's Programme or graduates of this form of training, which is crucial for the preparation of future commanders within the Romanian Armed Forces structure.

Table 1: Sample analysis in terms of work experience (author's design)

Years of experience	10-15 years	16-20 years	21-25 years	Over 25 years
Number of participants	29	32	10	2

As part of this questionnaire, I also wanted to find out whether deception is part of military training. Respondents were asked to rate on a scale of 1 to 10 the number of times they had participated in exercises involving deception. A score of 10 represented an extremely high number, in almost every exercise they had participated in, and a score of 1, none. The resulting extremely low average – 2.16 – shows

a very low interest in including deception in the training activities of the Romanian Armed Forces.

Moreover, in Romania there is no such training course dedicated to deception. Even post-graduate military-specific training courses do not place special emphasis on disciplines specific to this phenomenon. Most major international actors, including Romania's main strategic ally, the United States of America, attach great importance to the concept and provide specialised courses for their own personnel. (Joint MILDEC Training Course/JMTC, 2024; Army Deception Planners' Course/ADPC, 2024; INTL653/Deception, Propaganda and Disinformation, 2024).

Deception has long been understood in the Romanian Armed Forces as the process of masking, mainly involving passive measures of concealment and camouflage. It was implemented from Soviet doctrine in the early 1950s, replicating the concept of *"maskirovka"*. Two regulations that were published in 2015 and 2021 attempted to change the paradigm of the use of deception in the Romanian Armed Forces, ensuring that this concept would be aligned with the vision of Western armies. However, they only provide a primary framework for planning and conducting deception operations. A new mindset that includes a greater focus on disruptive and deceptive actions would go a long way towards increasing the chances of operational success for the Romanian forces, especially as the indigenous ingenuity and creativity of the Romanian people are recognised.

ROMANIAN MILITARY THINKING

Deception has long been understood in the Romanian Armed Forces as the process of masking, mainly involving passive measures of concealment and camouflage. It was implemented from Soviet doctrine in the early 1950s, replicating the concept of "maskirovka".

RESEARCH METHODOLOGY

Thus, **the research question** that guided our study was: *What are the reasons why the Romanian military should place a greater emphasis on misleading operations?* Accordingly, **the main objective** of this paper was to sensitize the decision-makers of the Romanian military system on the need to deepen the field of deception as a combat power multiplier. I appreciate that generating an increased interest on this topic would imply substantial benefits for the Romanian Armed Forces in the defence of the national territory, having the potential to contribute significantly to the improvement of all three components of combat power: conceptual, physical and moral. (AJP-01, Allied Joint

Doctrine, Edition F, Version 1, 2022, p. 49). Thus, the answers to the main question were organised in the form of subchapters, each presenting arguments to ensure the achievement of the proposed research objective. The way in which they were presented was thematic, with several reasons grouped together under one broad theme in order to ensure the coherence of the scientific approach.

Moreover, as mentioned above, **the main target of the study** is the Romanian military decision-makers at all hierarchical levels. However, although the paper is not intended as a guide to the planning and conduct of deception operations, it may be useful to all military planners, as the motivations offered in response to the main research question have the potential to shape the way in which the deception of this type of personnel is reported during the planning process of military operations.

In relation to the proposed objective, **the study was qualitative**, attempting to capture the specific nuances of the need for greater integration of deception in the Romanian philosophy of planning and conducting military operations. Moreover, I used an **inductive approach**, attempting to draw a general conclusion based on the empirical observations made (Given, 2008, p. 429). I also emphasise the methodological coherence of the options presented above, as the literature recognises that qualitative research primarily uses inductive reasoning. (Leavy, 2023, p. 9; Creswell, 2023, p. 276).

In order to achieve the set research objective, I decided to use **both primary and secondary data.**

The **primary data** used were collected using questionnaire as the research method. In order to be consistent with the type of research, qualitative, I chose to use open-ended questions to support a better understanding of the phenomenon under study. The main role of the data collected through the questionnaire was to support the identification and definition of the research problem, as presented in the previous section.

As for the **secondary data**, they supported the inferential process in order to provide a coherent framework for identifying the main arguments leading to the fulfilment of the objective of this study.

By ensuring the ability to make comparisons and inferences with how the issue of deception is approached in other military structures, I believe that secondary data was a viable option for this study. The value of using this type of data in research is recognised in the literature. (Walliman, 2022, p. 102).

THE GROWING ROLE OF DECEPTION IN ROMANIAN MILITARY DOCTRINE – WHY?

The purpose of this chapter is easy to understand. It represents the result of the research carried out and expresses the arguments on the basis of which I believe that the Romanian Armed Forces should give a higher degree of importance to the role that deceptive actions play in the conducted military operations. It is organised in a logical form, following an approach in which several similar arguments have been grouped thematically in order to provide a logical framework leading to the proposed objective of raising awareness among decision-makers in the Romanian military system of the need to further develop the field of deception. *Figure 1* highlights **the main themes** that emerged from the research conducted.

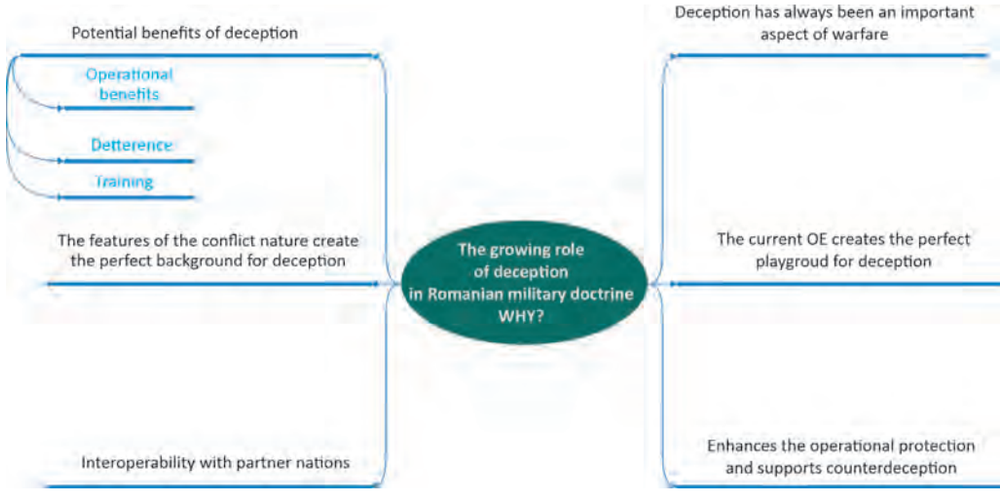


Figure 1: Arguments on the increasing role of deception in Romanian doctrine (author's design)

Deception has been – and continues to be –
an extremely valuable weapon in armed conflict

The first argument is based on a historical perspective. Deception has proven to be one of the oldest and most powerful weapons in armed conflict (Friedman, 2017, p. 73). Time has shown that it has been an inherent part of armed conflict regardless of the historical epoch. There are many examples to support this claim. One of the oldest and most well-known examples dates back to ancient Greece. It is the famous Trojan Horse, staged over 3000 years ago for the Greek conquest of Troy. Unable to conquer the city by direct action, the Greeks resorted to ingenuity to change the conditions on the battlefield. Using this stratagem, the Achaeans were able to exploit the prejudices of the Trojans by introducing, under the guise of a gift, a huge wooden Trojan horse, which was in fact full of Trojan soldiers. They opened the city gates and facilitated the Greek victory.

Deception has been – and continues to be – an extremely valuable weapon in armed conflict. Deception has proven to be one of the oldest and most powerful weapons in armed conflict. Time has shown that it has been an inherent part of armed conflict regardless of the historical epoch.

Ancient Chinese history is littered with examples of the use of deception. The concept was considered crucial to the success of military operations and over time became part of Chinese culture. Today, the name Sun Tzu, the famous Chinese strategist, is synonymous with the idea of deception. His work, *The Art of War*, has been a source of inspiration for Chinese and other strategists for more than 2000 years, although it was not translated, interpreted and properly adapted into English until the early 20th century. Over the years, the value of this work has been confirmed countless times in the practice of warfare.

The well-known aphorism attributed to Sun Tzu – *"All conflict is based on deception"* – has proved its validity in most armed conflicts throughout history. The ability to manipulate your opponent's information system (Friedman, 2021, p. 113) by creating a false picture of the course of events that would lead him to make decisions and act unconsciously against his own interests, which is the very essence of deception, has determined great military commanders to resort to deceptive tactics to ensure victory. Thus, memorable examples of the use of deception are as follows:

- *Battle of Gaugamela* (331 BC) – Alexander Macedon;
- *Battle of Trasimene Lake* (217 BC), *Battle of Cannae* (216 BC) – Hannibal;
- *Defeat of the rebellion of the Gallic tribes led by Vercingertorix* (52 BC)*/Gallic Wars* – Julius Caesar;
- *Battle of Hastings* (1066) – William the Conqueror, Duke of Normandy;
- *Seven Years' War* (1756 to 1763);
- *Battle of Long Island* (1776) – George Washington;
- *Battle of Lodi/Lombardy* (1796) – Napoleon Bonaparte;
- *Siege of Yorktown – American Civil War* (1862) – Confederate General John B. Magruder;
- *Gallipoli Campaign* (1915)/First World War;
- *Battles of Beersheba-Gaza* (1917) and *Megiddo Offensive* (1918)/Second World War;
- *Operation Barbarossa* (1941)/Second World War;
- *Operation Mincemeat* (1943)/ Second World War;
- *Operation Bodyguard*, Fortitude-South, Fortitude-North (1944)/ Second World War;
- *Cuban Missile Crisis* (1962);
- *Operation El Paso* (1966)/Vietnam War;
- *Yom Kippur War* (1973);
- *Falklands War* (Falklands - 1982);
- *Operation "Desert Storm"*/Gulf War (1991);
- *Kosovo War* (1998 - 1999);
- *Annexation of Crimea*/War in Ukraine (2014);
- *Israel-Hamas conflict* (2021);
- *Ukrainian counter-offensive to take Kharkov* (2022)/Russian-Ukrainian conflict.

Moreover, the historical value of deception has been recognised by the great military thinkers as a constant in their works. Sun Tzu, Niccolò Machiavelli, Carl von Clausewitz, Antoine-Henri Jomini, J.F.C. Fuller, B.H. Liddell Hart, John Boyd, all emphasised to a greater or lesser extent in their famous works on the art and conduct of war the importance of surprise and misleading the enemy in order to achieve operational advantages on the battlefield.

The deceptive nature of the human race, the multitude of benefits that deception can bring to support military operations, as well as the fact that in most cases the success of such actions is almost guaranteed, as Barton Whaley also acknowledged in his famous study, *Stratagem: Deception and Surprise in War* (Whaley, 1969, p. 76), make deception an inextricable part of armed conflict.

It is the specific elements of the nature of the conflict that provide the proper framework for deception

It is well known that *"the nature of war is constant; it is its character that changes rapidly"*. (JDP 0-01, 2022, p. 7). Thus, conflicts contain both characteristics that have remained constant over time and changing characteristics that are influenced by the specific societal characteristics. Uncertainty, the human side of conflict or violence are recognised as perennial elements of war that cannot be completely eliminated. (Jonsson, 2019, pp. 29-34; AJP-01, Allied Joint Doctrine, Edition F, Version 1, 2022, pp. 7-8). Regardless of the historical period, they have been identified and have directly influenced the way warfare is conducted.

Uncertainty provides the perfect framework for the use of deception. Against this background, the possibility of manipulating the adversary's perception of the operational situation and influencing his actions in the wrong direction is increased, thus ensuring the materialisation of opportunities to gain operational advantages over him.

Uncertainty provides the perfect framework for the use of deception. Against this background, the possibility of manipulating the adversary's perception of the operational situation and influencing his actions in the wrong direction is increased, thus ensuring the materialisation of opportunities to gain operational advantages over him.

With regard to **the human side of conflict**, as long as the military decision remains a human attribute, it is subject to error and can therefore be influenced by exploiting its limitations and vulnerabilities. Thus, shaping an adversary's perception and consequently his understanding of the battlefield situation (Friedman, 2017, p. 76) in order to induce him to take actions to his detriment remains a constant element of armed conflict.

The current environment creates the conditions for successful military deception operations

While the nature of armed conflict is unchanging, its character has transformed over time. The societal characteristics of each era have inevitably influenced warfare. For this reason, understanding the operational relevance of deception in the current context cannot be achieved without reference to the characteristics of the current operating environment.

Today, accurate information has become increasingly difficult to distinguish and obtain. This is a paradox of our times, where sensor technology for collecting information has grown exponentially. However, the sheer volume of data, the speed at which it is transmitted and the relative anonymity within social networks make it increasingly difficult to distinguish between fact and fiction, truth and falsehood. Against this backdrop, it has become increasingly difficult to detect and counter deception actions, namely disinformation. Now more than ever, given the growing importance of accurate and timely information, *"the entity that is able to generate the information advantage over the adversary is in a position to gain the initiative"* (AJP3.10.2, 2020, p. 1), a critical element of operational success.

Today, the technology of intelligence gathering has advanced to the point where almost total transparency of the battlefield has been achieved. Long-range targeting technology has also improved dramatically, as has the accuracy of these capabilities. However, the cost of such weapons is extremely high.

Technology has been and will continue to be the main vector for adapting battle tactics (Piehler, 2013, p. 362). We have witnessed an unprecedented technological development over the past decades, which has affected all sectors of society, including the military. Today, the technology of intelligence gathering has advanced to the point where almost total transparency of the battlefield has been achieved. Long-range targeting technology has also improved dramatically, as has the accuracy of these capabilities. However, the cost of such weapons is extremely high.

From the above observations, it can be seen that deception is becoming a crucial element in the conduct of conflicts in order to maintain a high level of combat capability. For example, the use of decoys can support the realisation of multi-spectral protection of forces and assets in today's transparent environment. In the ongoing conflict in Ukraine, false replicas of capabilities obtained from Western

allies have been widely used by the Ukrainians to ensure that they maintain a high level of combat capability in the face of the Russians.

In addition, false targets can be used to induce the adversary to waste expensive capabilities to destroy them, thus contributing to the degradation of their combat power. There are countless examples of sophisticated Russian equipment being fooled by decoys. Recently, an Internet video showed a Russian Iskander missile worthing about three million dollars engaging a Patriot launcher that was actually an inflatable replica. (X, 2024).

The value of these fake targets for the conduct of the conflict in Ukraine is also underlined by the attention paid to their development. For example, the company Metinvest specialises in producing replicas of combat equipment for the Ukrainian armed forces. (The Jerusalem Post, 2023).

With the development of technology and the increasing reliance of military forces on technology, electronic deception has become an extremely important weapon that can provide the framework for realising operational advantages on the modern battlefield.

In addition, with the development of technology and the increasing reliance of military forces on technology, electronic deception has become an extremely important weapon that can provide the framework for realising operational advantages on the modern battlefield. To achieve this, however, it is necessary to gain superiority over the adversary in terms of signature management. (Ryan, 2024).

In today's information age, the cognitive domain is becoming increasingly important (Weissmann, 2023, p. 271). Actions specific to this environment include degrading, disrupting, and influencing the adversary's cognitive capabilities in order to gain operational advantages over the adversary. (NATO Cognitive Warfare Exploratory Concept Draft, 2022, p. 3). Since deception involves manipulating the enemy's mind (Jasper, 2023, p. 1), it takes on new dimensions in today's operational environment.

Deception remains an extremely valuable element at the operational level. The most telling example dates back to the autumn of 2022, when, as part of the counter-offensive to regain lost territory in the Kharkov region, the Ukrainians managed to persuade the Russians to move the bulk of their forces to the southern front in the Kherson area, amid false Ukrainian signals of a possible attack in that area. This move facilitated the possibility of recapturing some 3000 km^2 in the Kharkov region. (Santelises, 2022).

Ensuring interoperability with allied forces

The undeniable value of deception in the current operational environment has been recognised by most of the major players on the global scene, some of them strategic allies of Romania. This is an additional argument for the Romanian Armed Forces to increase its interest in this type of operations. The reason for this is as simple and intuitive as possible: interoperability. In a context where Romania is unlikely to conduct military operations independently, finding solutions to synchronise the way operations are planned and conducted with allies is one of the prerequisites for defending the national territory.

Against a backdrop of heightened global competition for power, Western actors have recognised the need to move from the counterinsurgency operations practiced for nearly two decades to large-scale operations. In this context, it is recognised that *"deception will be critical to operational success"*. (NATO Cognitive Warfare Exploratory Concept Draft, 2022, p. 43). However, this paradigm shift is fraught with challenges. In addition to those arising from the characteristics of the current operating environment outlined above, a major challenge is to relearn some of the essential elements of major conflict, such as deception. (The Economist, 2020).

Against a backdrop of heightened global competition for power, Western actors have recognised the need to move from the counterinsurgency operations practiced for nearly two decades to large-scale operations. In this context, it is recognised that "deception will be critical to operational success".

The interest of Western militaries in the field of deception is also reflected in the timeliness of their doctrines devoted to this topic. In *table 2*, I have listed these documents and their year of publication for some key players in the current strategic environment. Their recent publication underscores the increased interest in this area, and thus accentuates the importance of understanding how deception can have an impact in today's conflicts.

Table 2: Allied doctrines of deception (author's design)

Actor	Year	Doctrine
NATO	**2020**	*AJP-3.10.2 Allied Joint Doctrine for operations security and deception*, edition A, version 2, NATO Standardization Office.

Actor	Year	Doctrine
USA	2017	*JP 3-13.4 Military deception*, US Joint Chiefs of Staff
	2019	*FM 3-13.4 Army Support to Military Deception*, US Department of the Army
	2024	*ATP 3-13.4 Army deception activities tactics, techniques, and procedures*, US Department of the Army
UK	2018	*Army Field Manual – Warfighting Tactics Part 1: The Fundamentals*, UK Ministry of Defence – the first annex of this document is dedicated to deception in military operations

The new NATO Warfighting Capstone Concept/NWCC emphasises the need for NATO forces to out-think their adversaries in order to prevail in future conflicts. In this sense, given the nature of deceptive operations, they may be one of the solutions to achieving this goal.

The new NATO Warfighting Capstone Concept/NWCC emphasises the need for NATO forces to out-think their adversaries in order to prevail in future conflicts. In this sense, given the nature of deceptive operations, they may be one of the solutions to achieving this goal.

Increased interest in this type of action is also being shown by some actors, in particular the United States of America, in order to assess the operational capability of its forces to plan and conduct deception. (US Department of Defense Office of Inspector General, 2022).

I understand that, in the context of conducting military operations in a multinational framework, in order to ensure the level of interoperability with its allies, Romania will have to find solutions to be able to invest more in the field of deception. It would ensure its *"ability to act with them in a coherent and effective way to achieve common objectives"*. (AAP-06, 2021, p. 71). Measures are therefore needed to ensure all three components of interoperability: technical, procedural and human. (AJP-01, Allied Joint Doctrine, Edition F, Version 1, 2022, p. 71).

For example, in the event of a potential conflict at home, **deception could provide an operational respite** until NATO's main forces arrive, or **it could help maintain a high level of operational capability** by causing the adversary to act on false replicas of key capabilities.

ROMANIAN MILITARY THINKING

The potential benefits of deception

However, perhaps the most important reason why the Romanian Armed Forces should increasingly incorporate specific elements of deception into the way they plan and conduct operations is the multiple benefits that these actions can provide.

They can be divided into several categories. The most important, of course, are the **operational benefits**. From this point of view, deception is a highly volatile action which, if successful, offers numerous benefits. According to British doctrine, they fall into **four broad categories**: achieving surprise, ensuring operational security, freedom of movement and economy of effort. (AFM, 2018, pp. 3A-2).

However, it is important to remember that deception is only a force multiplier that shapes the battlefield. It can never fulfil the functions of a decisive operation. The role of the inclusion of deception is therefore to support the concept of the operation by materialising operational effects that ensure the framework conducive to the accomplishment of the established mission. They cannot exist in a vacuum and **are an integral part of the overall military operation**. Their role is to cause the enemy to make operational errors without realising it. Thus, **in support of the commander's concept of the military operation, deception can:**

- cause the enemy to reveal his combat equipment, his strengths and weaknesses and, perhaps most importantly, his future intentions;
- confuse the adversary by overloading his sensors for intelligence collection and analysis;
- contribute to reducing the enemy's combat effectiveness by causing him to use his forces and assets ineffectively.

It is important to remember that deception is only a force multiplier that shapes the battlefield. It can never fulfil the functions of a decisive operation. The role of the inclusion of deception is therefore to support the concept of the operation by materialising operational effects that ensure the framework conducive to the accomplishment of the established mission.

Since the target of any deception operation is the enemy commander, these actions can contribute significantly to degrading the adversary's *OODA (Observation, Orientation, Decision, Action)* cycle, thereby ensuring decisional superiority over the enemy, and thus gaining and maintaining the initiative on the battlefield. Decisional superiority involves *"the ability to understand, decide, act and evaluate faster and more effectively than the adversary"* (Tunnell, September-October 2022, p. 79) and contributes decisively to his losing the battle.

Planning deception is also an extremely complex process that requires a thorough understanding of all the elements specific to the adversary. It is necessary to understand both his operational situation, how he acts doctrinally in such cases, and the elements of how the adversary gathers and analyses information, how he makes decisions, and what particular cognitive aspects influence his decisions. Thus, by analysing the possibility of incorporating deception into military operations, **a mindset can be developed that is geared towards analysing the adversary in depth**, thus providing the prerequisites for identifying timely solutions to exploit his vulnerabilities, even if this is not done through deception.

Planning deception is an extremely complex process that requires a thorough understanding of all the elements specific to the adversary. It is necessary to understand both his operational situation, how he acts doctrinally in such cases, and the elements of how the adversary gathers and analyses information, how he makes decisions, and what particular cognitive aspects influence his decisions.

Moreover**, the use of deception is in line with most of the combat philosophies** adopted by the Romanian Armed Forces. The incorporation of deception thus offers significant advantages in the implementation of the manoeuvrist approach or the mission command concept. Moreover, deception is considered the most important way to surprise the enemy (FM 3-90 Tactics, 2023, pp. 19-1), which is one of the oldest, well-known and widely used principles of armed combat. Thus, given that the achievement of surprise is a desideratum of any military operation (ADP 3-13 Information, 2023, pp. 6-2), it is easy to understand the Romanian Armed Forces need to deepen deception.

A second set of benefits that **deception** can provide are peacetime benefits. In this respect, it **can contribute significantly to the deterrence of adversaries, but also to the enhancement of training levels.**

In terms of **deterrence**, one of NATO's key peacetime functions (NATO Strategic Concept, 2022, p. 1), deception, by concealing vulnerabilities and overemphasising strengths, can at the very least confuse the adversary and thus prevent the creation of conditions conducive to an attack by the adversary. Even the simple public disclosure of the fact that the military exercises carried out by the Romanian Armed Forces include specific objectives for the training of deceptive actions can cause confusion to the adversary and slow down his actions, making him analyse the operational situation for a longer time, for fear of not being deceived. So, I understand that the perception of things is much more important than the reality itself.

Another extremely important area where deception can be beneficial is in **training.** This is an essential part of combat capability, providing, along with other elements, the physical component of combat capability. (JDP 0-01, 2022, p. 24).

Because of the nature of deception operations, which involve identifying the enemy's vulnerabilities, cracks in his modus operandi that can be exploited, and often require much more critical thinking, even outside the box, and ingenious solutions to deceive the enemy, **deception trains the critical and creative thinking of the personnel involved in planning such actions.** This effect has a direct impact on force training, with the potential to ensure a high degree of rigour and depth across the full spectrum of military operational processes. It is also recognised that the application of creative and critical thinking is one of the principles of the operational process. (ADP 6-0 Mission Command: Command and Control of Army Forces, 2019, pp. 2-4 - 2-5)

Because of the nature of deception operations, which involve identifying the enemy's vulnerabilities, cracks in his modus operandi that can be exploited, and often require much more critical thinking, even outside the box, and ingenious solutions to deceive the enemy, deception trains the critical and creative thinking of the personnel involved in planning such actions.

Ensuring one of the preconditions for countering the deceptive actions of adversaries

An extremely important element is that developing the ability to mislead also provides protection against such actions by the adversary. The main prerequisite for countering deception is to understand how it works.

In addition, based on the extensive experience of Romania's and NATO's potential adversaries, Russia (ATP 7-100.1 Russian Tactics, 2024, pp. 2-2) and China (ATP 7-100.3 Chinese Tactics, 2021, pp. 1-10), it can be seen that the role of deception in Romanian operational art must be intensified in order to create the right conditions for countering it.

In addition to the ability to increase the chances of detecting the opponent's deceptive actions, the knowledge of how deception works also supports the counteraction in the fifth phase of the counteraction process, *"Operational Response"* (Toroi, 2024, pp. 186-187).

CONCLUSIONS

The process of adaptation is essential to the survival of any organisation, including the military one. For this reason, the importance of identifying the critical elements of how armed forces operate and the ability to achieve timely system transformation in relation to these challenges is a key prerequisite for success in armed conflicts. NATO, the world's largest politico-military organisation, insists that *"to maintain military superiority and prevail in future conflicts, Alliance forces must continually adapt, evolve and innovate"* (Framework for Future Alliance Operations, 2018, p. 22). Adaptation is directly related to organisational flexibility. Mental, procedural and organisational rigidity, reluctance to change, inability to correctly identify the operational requirements of the armed forces are elements that hinder an effective process of the military structures adaptation.

"To maintain military superiority and prevail in future conflicts, Alliance forces must continually adapt, evolve and innovate". Adaptation is directly related to organisational flexibility. Mental, procedural and organisational rigidity, reluctance to change, inability to correctly identify the operational requirements of the armed forces are elements that hinder an effective process of the military structures adaptation.

Within this framework, the present article is aimed to draw the attention of the Romanian Armed Forces leadership to the issue of deception and its importance in the current security environment. Furthermore, the main results presented in this study have highlighted the most important benefits that the Romanian Armed Forces could gain from these actions, emphasising the need to intensify the role of deception in the Romanian military doctrine.

BIBLIOGRAPHY:

1. AAP-06. (2021). *AAP-06, NATO Glossary of terms and definitions (English and French).* NATO Standardization Office.
2. *ADP 3-13 Information.* (2023). Washington D.C.: U.S. Department of the Army.
3. *ADP 6-0 Mission Command: Command and Control of Army Forces.* (2019). Washington D.C.: U.S. Department of the Army.
4. AFM. (2018). *Army Field Manual – Warfighting Tactics Part 1: The Fundamentals.* UK Defence Ministry.
5. *AJP-01, Allied Joint Doctrine, Edition F, Version 1.* (2022). NATO Standardization Office.
6. AJP3.10.2. (2020). *Allied Joint Doctrine for operations security and deception, edition A, version 2.* NATO Standardization Office.
7. *Army Deception Planners' Course/ADPC*. (2024), https://www.1stio.army.mil/Training/IO-Training/Army-Deception-Planners-Course-ADPC/, retrieved on 12 May 2024.
8. *ATP 7-100.1 Russian Tactics.* (2024). Washington D.C.: U.S. Department of the Army.
9. *ATP 7-100.3 Chinese Tactics.* (2021). Washington D.C.: U.S. Department of the Army.
10. Creswell, J.W., Creswell, J.D. (2023). *Research design. Qualitative, Quantitative, and Mixed Methods Approaches,* 6th ed. Los Angeles: Sage Publications.
11. *FM 3-90 Tactics.* (2023). Washington D.C.: U.S. Department of the Army.
12. *Framework for Future Alliance Operations.* (2018). Norfolk: NATO Allied Command Transformation.
13. Friedman, B. (2017). *On Tactics. A theory of victory in battle.* Annapolis: Naval Institute Press.
14. Friedman, B. (2021). *On operations. Operational art and military disciplines.* Annapolis: Naval Institute Press.
15. *Future Leadership*. (2020). Multinational Capability Development Campaign.
16. Given, L.M. (2008). *The SAGE Encyclopedia of Qualitative Research Methods,* vol. 1-2. California: Sage Publications.
17. Hays, M.G. (2020), lt.-col. *Convergence of Military Deception in Support of Multi-Domain Operations*. In *Theater Army in Multi-Domain Operations Integrated Research Project.* U.S. Army War College.
18. *INTL653 – Deception, Propaganda and Disinformation*. (2024), https://www.amu.apus.edu/course-schedule/details/?c=INTL653, retrieved on 22 May 2024.
19. Jasper, L. (2023). *Start with the End. Effect Measurement of Behavioural Influencing in Military Operations.* Hague: The Hague Centre for Strategic Studies.
20. JCN1/17. (2017). *Joint Concept Note (JCN) 1/17 Future Force Concept.* UK Defence Ministry.
21. JDP 0-01. (2022). *Joint Doctrine Publication 0-01 U.K. Defence Doctrine,* 6th ed. UK Defence Ministry.
22. *Joint Doctrine Note 1-19 Competition Continuum.* (2019). U.S. Joint Chiefs of Staff.
23. *Joint MILDEC Training Course/JMTC*. (2024), https://jfsc.ndu.edu/Academics/Joint-Information-School-JIS/Information-Division/JMTC/, retrieved on 22 May 2024.
24. Jonsson, O. (2019). *The Russian Understanding of War. Blurring the Lines between War and Peace.* Washington D.C.: Georgetown University Press.
25. Kean, C., Maj. (November-December 2022). *Conceptualizing Information Advantage using Boyd's OODA Loop*. In *Military Review*, pp. 109-115.

26. Kennedy, C.H., Zillmer, E.A. (2022). *Military Psychology. Clinical and Operational Applications,* 3rd ed. New York: The Guilford Press.
27. Leavy, P. (2023). *Research Design – Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches,* 2nd ed. New York: The Guilford Press.
28. *MCDP 1-4 Competing.* (2020). U.S. Marine Corps.
29. Mazarr, M.J., Blake, J.S., Casey, A., McDonald, T., Pezard, S.&Spirtas, M. (2022). *Understanding the Emerging Era of International Competition Through the Eyes of Others. Country Perspectives.* Santa Monica, California: RAND Corporation.
30. *NATO Cognitive Warfare Exploratory Concept Draft.* (2022). Norfolk: NATO Allied Command Transformation.
31. *NATO Strategic Concept.* (2022). Madrid: NATO.
32. Piehler, G.K. (2013). *Encyclopedia of Military Science*. Los Angeles: Sage Publications.
33. Ryan, M. (2024), https://mickryan.substack.com/p/the-quest-for-a-new-offensive-doctrine, retrieved on 12 June 2024.
34. Santelises, A. (2022), https://cove.army.gov.au/article/ukrainian-kharkiv-counter-offensive-and-information-operations, retrieved on 12 June 2024.
35. *Strategic Survey 2022. The Annual Assessment of Geopolitics* (2023). London: The International Institute for Strategic Studies, Routledge.
36. TC 7-102. (2014). *Training Circular No. 7-102 Operational Environment and Army learning.* Washington D.C.: Headquarters Department of the Army.
37. *The Economist*. (2020), https://www.economist.com/christmas-specials/2020/12/16/democracies-need-to-re-learn-the-art-of-deception retrieved on 11 June 2024.
38. *The Jerusalem Post* (2023), https://www.jpost.com/international/internationalrussia-ukraine-war/article-762030, retrieved on 12 June 2024.
39. Toroi, G.-I. (2024). *Enhancing operational protection: a step-by-step counter-deception guide*. In *Buletin Științific,* Academia Forțelor Terestre "Nicolae Bălcescu", Sibiu, no. XXIX(1), pp. 179-188.
40. Tunnell, C.H. (September-October 2022). Command Post Automation. In *Military Review*, pp. 79-86.
41. *U.S. Department of Defense Office of Inspector General* (2022), https://www.dodig.mil/reports.html/Article/3200866/project-announcement-evaluation-of-combatant-command-military-deception-plannin/, retrieved on 22 May 2024.
42. Walliman, N. (2022). *Research methods – the basics,* 3rd ed. New York: Routledge.

43. Weissmann, M., Nilson, N. (2023). *Advanced Land Warfare – Tactics and Operations.* Oxford University Press.
44. Whaley, B. (1969). *Stratagem: Deception and Surprise in War.* Center for International Studies, Massachusetts Institute of Technology.
45. *X*. (2024), https://x.com/Tendar/status/1788964161575116871?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1788964161575116871%7Ctwgr%5E772fe80018a0b64b0ab2815e69d01adb7662ce0b%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.digi24.ro%2Fstiri%2Fexterne%2Fcum-sa-irosest, retrieved on 12 June 2024.

ANALYSIS OF MULTI-DOMAIN OPERATIONS CONCEPT AND THE ROLE OF EMERGING ADVANCED AND DISRUPTIVE TECHNOLOGIES FOR ITS OPERATIONALISATION

Captain Ionuț-Iulian CĂLUGĂRU, PhD Student
"Carol I" National Defence University, Bucharest
10.55535/RMT.2024.3.5

At present, Multi-Domain Operations (MDO) concept is of interest for the whole defence and security sphere, especially for the Euro-Atlantic area, where its implementation and operationalisation are desired at the level of the military instrument of power, as well as at the national and international strategic level, in an allied and partner context.

The manner in which emerging and disruptive technologies can be transferred and integrated into the military field in order to provide stability and give the concept practical-applicable utility, and the way in which it can be operationalised, are elements of great interest to national military authorities at the moment, while giving the concept a probabilistic character for those analysing this area of the military field.

Moreover, the decision-making process and the operational side are elements that, in the multi-domain integrative framework, require the involvement of advanced technologies, in particular artificial intelligence, which also, as a subdivision of technology, practically marks the existence of the contemporary human being, becoming a basic constituent in the conduct of military actions.

In this article, we will try to give a realistic picture of this concept by presenting information analysed and extracted from bibliographical sources that reflect a qualitative and topical character. Therefore, the research method used throughout this paper will be the bibliographic research method (literature review), through which we will attempt to project a critical analysis of the impact that the concept will have on society.

Keywords: emerging technologies; artificial intelligence; multi-domain operations; decision supremacy; disruptive technologies;

INTRODUCTION

The term *modern battlefield* is used to give a transposition of ideas that are based on empirical elements from the past of armed combat, namely ideas about how military actions can be developed according to human and technological evolution. At the moment, the battlefield picture of the future is shaped around contemporary elements such as *artificial intelligence* and *multi-domain operations* and the way they can be integrated to gain decisional and actional advantage over the adversary. Therefore, the elements mentioned in the previous sentence also substantiate the necessity of the present study, knowing that the time and energy-consuming concern among political and military leaders has always been focused on achieving superiority over the adversary.

Disruptive and emerging technologies have occurred as a response to the evolution and development of subsidiary branches of technology such as artificial intelligence, digitalisation, machine learning etc., having a decisive impact on all societal domains, including the military sphere, where the battlespace and, ultimately, the conduct of combat have acquired new facets.

The rationale behind this article is the need to understand the impact that artificial intelligence can have at the decision-making level and, even more, at the action level. Technologization is a product of the progress that mankind has made in all spheres of its existence, driven by the desire to dominate in a particular field, practically to take the lead in various competitive areas such as industrial, political, military, economic etc. Disruptive and emerging technologies have occurred as a response to the evolution and development of subsidiary branches of technology such as artificial intelligence, digitalisation, machine learning etc., having a decisive impact on all societal domains, including the military sphere, where the battlespace and, ultimately, the conduct of combat have acquired new facets. Here we refer to the expansion of the battlespace as the physical barrier has been overcome, time has become compressed and the speed of information transmission has increased, making it almost imperceptible, thus creating the conditions for new concepts such as *Multi-Domain Operations (MDO)*.

The purpose of this study is to provide a clear picture of the way emerging technologies and artificial intelligence, as a subsidiary,

are being integrated and used in military operations, particularly in multi-domain operations, and, in more detail, of the decision-making dimension at each of the three levels of military operations: strategic, operational and tactical. The concept of artificial intelligence becoming an essential element of military operations is at this point a goal that is most likely easily achievable. The completeness of the fact that both current and future emerging and disruptive technologies will result in the link between military and non-military aspects, generating, in effect, a new and more complex physiognomy of armed combat, and shaping this integrated multi-domain framework, is of a self-evident character, concretised by the research already in place.

Artificial intelligence can be used to achieve decisional and actional supremacy over the adversary. Starting from this working hypothesis, throughout this article, we will try to highlight those aspects through which artificial intelligence finds its usefulness in the process of military operations and also to understand what the role of the military leader is in this process, considering the characteristics that systems, which are based on this branch of technology, possess.

The hypothesis behind the present study refers to the fact that artificial intelligence can be used to achieve decisional and actional supremacy over the adversary. Starting from this working hypothesis, throughout this article, we will try to highlight those aspects through which artificial intelligence finds its usefulness in the process of military operations and also to understand what the role of the military leader is in this process, considering the characteristics that systems, which are based on this branch of technology, possess.

The most recent and complex studies highlighting the contribution and necessity of implementing advanced technologies in multi-domain operations are carried out by the most economically and militarily developed countries, including the United States of America (USA), the United Kingdom (UK), France, Spain and, even at the organisational level, the North Atlantic Alliance (NATO) or the European Union (EU). They have conducted research on this novel element, generating documents at the conceptual level to reinforce the idea that the achievement of a reliable multi-domain level system is a necessity for future politico-military action. While there are relatively new elements under our analysis, there are some scriptural and already known milestones that literally and theoretically lay out how the concept of multi-domain operations is presented at this time, such as *The U.S. Army in Multi-Domains Operations 2028* (US Army, 2018), *A Strategic Compass for Security and Defence For a European Union that protects its citizens, values and interests and contributes to international peace and security* (European Union External Action, 2022) or *Allied Joint Doctrine* (NATO Standardization Office, 2022). These are milestones of what multi-domain operations mean on the international stage, the basic idea issued at the level of the United States of America being quickly taken up by the allies and, even, by the organisations to which they belong. With regard to artificial intelligence and its applicability in the military sphere, we find a series of views shared by various authors, in particular, *Military Applications of Artificial Intelligence* (Morgan et al., 2020) or at state level by the Ministry of Defence of the United Kingdom through the *Defence Artificial Intelligence Strategy*, which outlines both the importance and the vision of the use of artificial intelligence in the military organisation.

From a methodological point of view, in this study, we will focus on the use of the bibliographical method by analysing and extracting the elements we need, using specialised and relevant documentation in the field of interest. We will also aim to obtain and issue a material based on the quality of the information obtained, given the dimensions imposed by the nature of this study, in relation to the complexity of the problem under investigation.

The future will bring even more novel elements, at a much faster speed than we might be used to, which will be due to the unprecedented development of not only technology but also the human being.

The end of the introduction complements the idea that the future will bring even more novel elements, at a much faster speed than we might be used to, which will be due to the unprecedented development of not only technology but also the human being. In the future, man, by his very nature, will be a fighter who will perpetually try to impose himself in his sphere of interest, so, depending on the size of the space over which his influence extends, even the methods by which he will seek to achieve the status of dominator will differ, the ultimate act being war itself.

DEFINING ELEMENTS OF MULTI-DOMAIN OPERATIONS CONCEPT

In a pluralistic society, such as we find in democratic states today, leading each member of society towards a common vision, specific to a particular ideology, creates constant challenges for the political system and for the structures whose mission is to consolidate societal values. Achieving a secure and stable environment is hampered, firstly, by the hostile intentions of some state and non-state actors and, secondly,

by the very diversity of society, with imbalances generated by different ideologies, such as political, ethnic or sexual. Beyond the military aspects of Multi-Domain Operations, the concept has an integrative role in harmonising the military – non-military framework, which gives shape to the whole idea behind the concept. A likely result of the implementation of this concept at national level can be found in the acceptance of the individual as a provider of security and as an integrated part of the military operation process.

Providing an overview of the definition of the MDO concept, in relation to the dimensions required by this paper, will further include a theoretical approach by presenting some defining elements of the connection between this concept and its spheres of influence, in this case military, national and international.

Beyond the military aspects of Multi-Domain Operations, the concept has an integrative role in harmonising the military – non-military framework, which gives shape to the whole idea behind the concept.

Adapting the military architecture to the requirements of the MDO concept is the main point of interest, at the same time taking into account that a multi-domain operational framework is optimal to be able to respond to today's threats. Even if the basic premises refer to a single whole made up of the harmonisation of military and non-military structures, the scope of action is much more complex because, beyond the capabilities available at national level, the North Atlantic Alliance wants a multinational interaction; moreover, even partner states can be included in this whole with a focus on achieving established objectives. In the same vein, we add the view of the UK Ministry of Defence, which states that conceptual inoculation at defence system level is desired, but with the support of the *"Whole Force"* (Ministry of Defence, Multi-Domain Integration, 2020), further defining the term as the involvement of active military personnel, reservists, civil servants and industry structures to strengthen defence. This aspect reinforces the point made in the first paragraph, namely that the entire society becomes part of the multi-domain whole, making its necessity a reality.

From a military point of view, this concept will be integrated at all levels of military operations (strategic, operational, tactical), being a condition and a desideratum in relation to their interdependence. While the strategic level deals with politico-military aspects, the operational and tactical levels emphasise the military side, where military capabilities are actually deployed to achieve the objectives established on the strategic-operational-tactical pendulum.

At national level, the concept of multi-domain operations and the possibility of its integration depends on non-military variations and the adaptability of the entire defence system, with reference to all its component structures. For a better understanding, we offer the concrete example found in the *Military Strategy of Romania* where *Integrated Joint Force* is defined (MApN, 2021, p. 25) as the concept underlying the way the armed forces operate in an inter-institutional environment in order to achieve established objectives. Starting from the definition of the two concepts, *Integrated Joint Force* and *Multi-Domain Operations*, we can state that from a national point of view, the concept of Multi-Domain Operations aims to include all the elements that have the capability to act together with the armed forces to develop actions necessary to achieve specific objectives or missions.

The approach to Multi-Domain Operations concept by transposing it internationally, taking into account the multitude of factors that can influence the directions of implementation and integration, is a complex one.

The purpose of initiating this concept is relatively easy to understand, aiming to achieve a balance of power between the two poles of power in the international sphere. Using the elements in a practical way to achieve the desired results must be underpinned by an integrative framework between the theoretical aspects and the physical capabilities that can serve this purpose. The problem is imposed by the lack of the necessary infrastructure at international level to demonstrate in real terms what this objective is aiming at. By using the term *international*, we are referring to inter-state cooperation, which first of all requires the implementation of multi-domain notions in national doctrine in order to achieve the inductive meaning that starts from the particular and ends with the general, depending on the defining elements that delimit the terms national and international.

The states that have begun to take a comprehensive analysis of the MDO concept will most likely be the first to succeed in establishing a pluri-domain framework at multinational level for joint action at tactical and operational level, whether in military exercises or in response to a real threat.

The states that have begun to take a comprehensive analysis of the MDO concept will most likely be the first to succeed in establishing a pluri-domain framework at multinational level for joint action at tactical and operational level, whether in military exercises or in response to a real threat.

Aspects relating to the development of capabilities or the integration at doctrinal level of the ideas set out in the MDO concept provide the rhythmicity of its operationalisation process, depending on the capacity of each individual state, the way in which the end state will look like, where the ideal is rendered by integration at military, national and international level.

IMPACT OF EMERGING AND DISRUPTIVE TECHNOLOGIES ON MULTI-DOMAIN OPERATIONS

Through communication and information access channels, specifically the internet, we are given a plethora of details about the latest developments in technology, whether we are referring to robots displaying human traits (United Nations, 2023) or to the capabilities of the cyber domain, where the human resources have been replaced with humanoids, the outcome of the progress of artificial intelligence, capable of presenting news programmes, exclusivity being offered to the public by China (gadget-talk. ro, 2018). Although the non-military environment is leading the technological field, this need for development is also felt in the military sphere, which is why the interconnection between the military and non-military areas must exist, a fact confirmed by the defining notions of multi-domain operations which, in fact, represent a synchronization of military and civilian activities on an inter-domain level (Allied Joint Doctrine, 2022, p. 2).

With the innovations that have emerged in the military field, the practical-applicative side has taken another turn, which requires the doctrinal area to take steps to bring the doctrinal-technical framework into balance.

In recent years, new areas, such as cyber and outer space, have been added to the already established military operations domains (land, air and sea) and their relevance has become increasingly prominent. Over the years, they have been displaying new techniques and equipment aimed at dominating the field and even the battlespace. New technological developments, which have emerged as a quantitative and qualitative response to the information acquired by human beings in the course of history and the revolutionary periods it has witnessed, are increasingly making their mark on the military field as well, with particular emphasis on military science and art. With the innovations that have emerged in the military field, the practical-applicative side has taken another turn, which requires

the doctrinal area to take steps to bring the doctrinal-technical framework into balance. The fundamentals of military science will remain the same, here referring to the laws and principles of warfare, which are universally valid, but the way in which the process of operations will relate to them will differ; it is because essential elements such as space and time are *"altered"* in relation to the traditional elements that are already known according to the physical domains. Overcoming these physical limits of the already established domains of operations is a result of these emerging and disruptive entities that can give the possessor an advantage in decision and action.

What Emerging and Disruptive Technologies Are

In order to better understand the subject, the next part of this paper will provide a brief presentation of the technologies in terms of their emerging and disruptive nature, resulting in an introductory part towards their use in the military environment, in relation to the new concepts promoted.

Cambridge Dictionary defines emerging technology as a new technology that completely changes the face of things, or in other words, offers a new perspective on how to approach them. In the non-military environment, the term disruptive technologies is not new, having been mentioned as early as 1995 by Clayton M. Christensen and Joseph L. Bower in an article published in *Harvard Business Review* (Christensen and Bower, 1995), referring to technology in corporations. Since then, things have evolved and, of course, the notion has found even more industrial applicability to markets and society in general.

Cambridge Dictionary defines emerging technology as a new technology that completely changes the face of things, or in other words, offers a new perspective on how to approach them. In the non-military environment, the term disruptive technologies is not new, having been mentioned as early as 1995 by Clayton M. Christensen and Joseph L. Bower in an article published in Harvard Business Review.

At the military organisation level, in addition to the stream of novelty of an applicative-practical nature coming from the civilian area, there is also the notional part, which of course premeditates the emergence of physical elements and which submits this system to a deeper analysis of the doctrinal perspective, having to adopt, in the end, measures to adapt the concept, necessary to maintain the balance between novelty and actuality. Related to the general idea of this paragraph is the syntagm *disruptive military technology* that, as defined by the national security specialist Niculae Iancu (2019), *"is an improved or completely new technology capable of producing*

fundamental changes to traditional security and defence models". Disruptive technologies that will find their application in the military, whether at the strategic, operational or tactical level, are artificial intelligence, autonomous weapons systems, quantum technology etc., elements already established at various international congresses, such as the Munich Security Report 2022. The fact that ten years ago we were discussing issues that seemed to be in the realm of the fantastic, which existed only in theory, gives even more freedom to the imagination in the years to come, and just as in the military environment time in units of measurement has become much more compressed, for example in the transmission of information, so it is in the case of technological developments, with the time to materialise the finite products of this infinite field becoming ever shorter.

The initiator of the Multi-Domain Operations concept is the United States of America, which in 2018 published The US Army in Multi-Domain Operations 2028, which aims to maintain the advantage and even defeat a potential enemy, almost equally.

Probably, a large part of the current emerging technologies, as well as those that will be discovered in the years to come, will find their use in the military field, but, nevertheless, beyond the question of their use and their integration into the military operation process, it is also necessary to mention the economic-financial issue which, in the end, is the driving force behind research in each field and which also contributes to the differentiation between strong and politically-militarily developed states and states that do not have all the necessary resources.

Disruptive Technologies and Multi-Domain Operations Correlation

The initiator of the Multi-Domain Operations concept is the United States of America, which in 2018 published *The US Army in Multi-Domain Operations 2028*, which aims to maintain the advantage and even defeat a potential enemy, almost equally (US Army, 2020, p. 3). The implementation at the national level of this concept is intended to cover the full spectrum caught by the definition of conflict, from peacetime to actual war and back to competition under favourable conditions.

In order to start such a process whereby inter-domain action is possible in real time, it is necessary to have capabilities in the sphere of those classified as emerging, because only through a high degree

of technologization can such interconnection be achieved. This aspect of state capabilities and capacities, in the global context, imposes barriers in the implementation of this concept, which is why some state actors are still at an early stage of empirical and even conceptual approach as well as transposition at the level of their own security and defence system.

Achieving this operational framework on a multi-domain and, why not, all-domains level requires time, human and material resources, where we bring advanced technologies to the fore. The characteristics of all these listed elements can lead to the construction of a multi-domain environment where forces can safely perform their missions. With the USA taking a public stand on multi-domain operations, a broad process of capability development has begun, encompassing artificial intelligence, robotics, hypersonic weapons, unmanned drones etc. (The United States Army War College, 2020, p. 21), which is changing the *"face"* of warfare as known to mankind to date.

In this environment, the complexity of warfare is increasing, the way of fighting will be influenced by aspects such as new capabilities that will be developed and introduced into combat to highlight the principle of enemy surprise, the diversity of forces and their mode of action, with contemporary society witnessing the unconventional way of fighting from extremist groups in Afghanistan. Mobility is another feature influenced by technological development, with the war in Ukraine providing a good example of freedom of movement through capabilities deployed and controlled remotely without the physical involvement of human resources on the battlefield.

Mobility is another feature influenced by technological development, with the war in Ukraine providing a good example of freedom of movement through capabilities deployed and controlled remotely without the physical involvement of human resources on the battlefield.

The human evolutionary result of empirically accumulating and acquiring knowledge when referring to the politico-military framework and the conduct of operations is the recognition of the cyber and space domains as operational domains. These two domains cannot function without the existence of emerging technology, or in other words, they can only exist at an a priori level, without giving man a tangible experience. Sustaining and keeping them operational strictly depend on technological development and on obtaining the necessary resources to be able to maintain the necessary technical support.

As known history tells us that human beings are moving towards progress, we will certainly witness new scientific breakthroughs in the future, the scale of which will be transposed both cyber space and outer space.

The role of such technologies is to create a stable interconnection across the five recognised operational domains. In practical terms, they will facilitate communications, the transmission of information in real time, and the connection between the command-and-control elements of the operational and tactical echelons with the forces on the battlefield, in an inter- and intra-domain framework. It is not only time that will become compressed in this multi-domain climate, even space will change in that any action will be known at any location on the globe, and long-range strike capabilities can cover areas of operations with their range, no matter what the battlefield looks like.

The role of such technologies is to create a stable interconnection across the five recognised operational domains.

At this level we have an overview and a perspective between the major military players, including the United States of America, the People's Republic of China, the Russian Federation and, at alliance level, the North Atlantic Treaty Organisation, which is promoting a revolutionary competition for supremacy in the economic, political and military spheres. I mention the term perspective because in the years to come, we will most likely have the same major state actors on the international stage, which will be in constant competition to develop their own capabilities.

In practical terms, they will facilitate communications, the transmission of information in real time, and the connection between the command-and-control elements of the operational and tactical echelons with the forces on the battlefield, in an inter- and intra-domain framework.

THE ROLE OF TECHNOLOGY IN ENSURING BATTLEFIELD SUPREMACY

In this chapter we aim to highlight, as the title suggests, how technology, as a general term, can influence the information dimension of warfare and also the implications for decision-making and action. We will also turn to documents issued at the level of the North Atlantic Alliance and by the United States of America, as well as various scholarly works by authors with expertise in the field of study.

In the development of this chapter, we will start by saying that information superiority will lead to decisional supremacy (Perry et al., 2004, p. 3). The first element analysed will be informational superiority, as information is an indispensable element in all fields and it has been

demonstrated in many situations, as well as at the societal level, that the holder of information can develop actions with unpredictability. From a military point of view, in order to be at an advantage on the battlefield, it must be possible to obtain real information about the adversary's capabilities, his position in the field or the tactical field, which is why informational battlefield analysis is such an important step in the decision-making process (Wade, 2020, p. 3-3).

The technological progress has definitely influenced the possibility of working with information with the architectural development of C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Research) by the United States of America, specifically at the directive of the Assistant Secretary of Defense who argued that more effort is needed for C4I to provide for the warfighter's needs to accomplish the mission (Architecture Working Group, 1997, pp. 1-2). Thus, this initiative resulted in the first version of C4ISR in 1996, which is an integrative system that, at that time, was aimed at gaining advantage over the adversary, situational and battlefield awareness, and reducing the time between target discovery and taking action. Technological evolution has helped the military system to reach the C4ISR moment, an architecture that has optimised the transmission and use of information for the benefit of its forces.

From a military point of view, in order to be at an advantage on the battlefield, it must be possible to obtain real information about the adversary's capabilities, his position in the field or the tactical field, which is why informational battlefield analysis is such an important step in the decision-making process.

The features of the modern battlefield are constantly changing, its physiognomy is acquiring a new meaning, and new methods are being sought to confront the unpredictability created by the enemy. The aim is to combat the elements that give surprise with the same style of work, a lesson that can be seen to have been learned from past conflicts and wars. As mentioned in the previous chapter, Afghanistan, with the groups that caused instability during the missions carried out by NATO member states on its territory, gave the North Atlantic Alliance, and the United States of America included, the opportunity to learn and to take on board certain lessons. In extenso, we refer to the Taliban insurgency acting against the Western armed forces present on Afghan territory and also to the way in which they used hybrid-type elements and, more often than not, improvised devices to attack certain military structures. These are factors that have led to new conceptual approaches, such as multi-domain operations,

in the idea of countering the element of surprise. Of course, in this regard, we have several causes for the desire to implement and operationalise the concept, among which we mention the military and economic development of competing states, namely China and Russia, which have brought to the fore anti-access and area denial systems (Anti-Access Area Denial A2/AD) (Perkins, 2018). The idea that we want to put forward focuses on the creation of compatible systems at the level of all categories of forces and also inter-domain and intra-domain, which can be used to repel threats of any kind, mainly to the security of the Euro-Atlantic area.

The technological derivatives that will be implemented at all three levels of operations – strategic, operational and tactical, in the circumstances offered by the multi-domain complexity, will aim to favour the decision-making process and, ultimately, the operational process by revolutionising the space-time spectrum in all its singularity, in the five established operational domains: land, air, maritime, cyberspace and space.

The technological derivatives that will be implemented at all three levels of operations – strategic, operational and tactical, in the circumstances offered by the multi-domain complexity, will aim to favour the decision-making process and, ultimately, the operational process by revolutionising the space-time spectrum in all its singularity, in the five established operational domains: land, air, maritime, cyberspace and space. *Space and time,* immaterial but brought to the level of resources in the military operational process, require evolutionary approaches to optimise, in practice, what we consider to be quantified by units of measurement. Thus, technology and this multi-domain framework offers the opportunity to unify actions precisely to cover an as large as possible area in an as short as possible period of time, components that will enable command and control elements to make the best decisions and to act accordingly. In this way, the aim is to improve the process of operations in terms of *planning, training, execution* and *evaluation*, in the integrative context of multi-domain operations.

The conduct of military operations has been based on intelligence, in the sense that as long as more details about the adversary and the battlefield are known, forces can be adequately prepared and finally given the opportunity to take the initiative on the battlefield. This element has remained fundamental to the military operation for each of the combatants. The challenge is how the information can be obtained and how quickly it can be analysed and transposed into an operational plan. The collection of data and intelligence is facilitated

at this point precisely by contested domains such as cyber (Ross et al., 2021, p. 23), which create opportunities for cyber attacks whose origin cannot be identified. The vastness of this domain also requires technological development and ultimately digital development to match. As mentioned throughout this paper, technologization is closely linked to economic and financial development, initially being tested in the non-military area, and then elements deemed necessary to the military apparatus become contracted.

However, technologization, beyond its benefits, also brings destabilising factors that are difficult to control. In other words, the exposure offered by the digital age in which we find ourselves, also provides an opportunity for non-state actors (Cyberspace Operations, 2018, p. I-2) to make their presence felt in the military sphere, and not necessarily in a positive sense. The cyber domain is the most exposed to such threats, precisely because it cannot be controlled. After all, it is a domain without limits, or if they are imposed, they cover a small spectrum or rather are meant to provide protection against external threats, which is why malware is also used. These malware attack enablers operate on the basis of abstract elements, which differentiates the cyber domain from other infrastructure-based physical domains, as there are also man-made physical elements within the space domain, such as probes, space stations or various technologies that are in outer space.

Technologization, beyond its benefits, also brings destabilising factors that are difficult to control. In other words, the exposure offered by the digital age in which we find ourselves, also provides an opportunity for non-state actors to make their presence felt in the military sphere, and not necessarily in a positive sense.

Using advanced technologies for cross-domain operations is still a challenge that is generated not only by the competition between state actors with capabilities in this regard, but also by the aforementioned non-state actors, independent or affiliated to organised crime groups that, in return for various benefits, try to cause instability in different environments, especially in the cyber domain, which at the moment is likely to be the most vulnerable.

In the next part of this article, we will analyse how artificial intelligence, as a subdivision of the technological complex, finds its usefulness in the military operation process. This sub-chapter complements the picture that this study seeks to present, that of the use of new technologies in the military environment and, as such, in a multi-domain context. The data provided in this article are intended

to generate a deductive perception of the central idea, starting from the correlation between emerging and disruptive technologies and multi-domain operations, continuing with the impact of technology on the information environment and how the transmission of information can be facilitated, and finally looking at how artificial intelligence manages to be integrated into the operation process, as mentioned in the introductory part.

IMPLICATIONS OF ARTIFICIAL INTELLIGENCE IN THE DECISION-MAKING PROCESS

Interstate competition at the political, economic, and military levels among the major global powers is fierce, in particular, bringing to the fore the state of competition between China and the USA, with the former having the capacity to become the strongest rival, according to *The US Army in Multi-Domain Operations 2028* (US Army, 2020, p. 3), in the areas listed at the beginning of the paragraph. China has the capabilities to develop not only in the economic sphere to an even greater extent than it does today, with the *Bloomberg* website ranking it as the world's second largest economy after that of the United States of America (Miller, Curran, 2024), but also in the military sphere where it is making considerable progress. All these aspects are an implicit result of the technological factor, and the two mentioned major state actors are succeeding in revolutionising the technological field with resonance on the military environment too. Thus, emerging technologies such as artificial intelligence have an impact on the way the armed combat will be conducted and the battlefield will look like in the future.

Artificial intelligence is an intensively used concept at societal level, being to a large extent present in everyday life, supporting human actions, but at the same time reflecting a potential threat to human security, for example through possible leaks of sensitive information.

Artificial intelligence is an intensively used concept at societal level, being to a large extent present in everyday life, supporting human actions, but at the same time reflecting a potential threat to human security, for example through possible leaks of sensitive information. However, an improvement of this sector, represented by intelligent capabilities, is under constant development, with each individual state wishing to adapt its infrastructure in such a way as to be able to achieve as many positive results as possible through the use of these technologies. For its part, the military sector, being the main provider

of security and safety for the population, is taking steps to implement it at the level of its capabilities in order to achieve speed of reaction in decision-making and increased capacity for action when the situation requires it.

Regarding the use of artificial intelligence in the development of military capabilities, the greatest progress in this regard is being made by the United States of America, but China is also close behind (Kania, Costello, 2018, p. 2). The competition over the development of technologies is, on the one hand, beneficial because it tends to lead humanity to another level of comprehensibility, in a new information age, with the aim of filling in the gaps in the vast *puzzle* of knowledge. However, on the other hand, the same process of technological development may also have repercussions in terms of the escalation of a possible conflict between the major powers, and even if we stop at the cyber sphere, there will still be actions that will have repercussions on the population and the whole security system, because of the volatility of this area.

The competition over the development of technologies is beneficial because it tends to lead humanity to another level of comprehensibility, in a new information age, with the aim of filling in the gaps in the vast puzzle of knowledge.

In terms of decision-making, the use of artificial intelligence is intended to help military leaders make the right decisions by optimising data and processing speed. In practice, the aim is to provide a real-time picture of the battlefield, increasing commanders' knowledge of the situation of troops or their disposition in the field and their material state. The decision precedes the action, which is why we believe that, if a decision is correct and taken in a short time, then the action is likely to have the same effects. Hence, from this we can also extract the usefulness of artificial intelligence in the decision-action correlation, excluding the possibility of its use in the physical field through various technical means that can drive actions to achieve goals without human assistance or through remote guidance.

Artificial intelligence is considered to have the potential to erode the state of stability of the security environment, practically altering inter-state relations, and here we refer to the competitive framework, by bringing to the fore the risk prone to surprise attack (Davis, 2019, p. 14). In the same line of thought, referring to all three levels of the military art – strategic, operational and tactical – it must be identified at which level there are potential risks launched by systems that have

artificial intelligence as their operating model. It is relevant to talk about the operational and tactical level and the impact of artificial intelligence on them, but, in fact, a basic framework is created in an axiomatic level, given that the battle is directed within these two levels, and the speed of action is an essential element of the confrontation, hence the need to make timely and correct decisions. On the other hand, given the scale of the strategic level, where we include the political factor, artificial intelligence may not produce the same element of surprise, a point also suggested by James Johnson in his book *AI and the Bomb* (Johnson, 2023, p. 236). The scale and implications of this level as well as the drivers of decision-making are difficult to control under AI. The fact that we can capture, according to the definition of levels, decisions taken in the decision-making process as a result of the effects achieved by actions taken at strategic and operational level reveals a representation of a cause-effect cycle and not of direct implications.

In a multi-domain context, the applicability of artificial intelligence in decision making and action taking is to quickly transmit information, synthesise it and finally provide it to leaders to make the best decisions.

In a multi-domain context, the applicability of artificial intelligence in decision making and action taking is to quickly transmit information, synthesise it and finally provide it to leaders to make the best decisions. The complexity, however, is rendered by the connection it must create at a multi-domain level to meet the needs that fulfilling a mission requires. Interoperability between at least two operational domains is essential according to the concept, and the integration of non-military factors into military operations implies a high degree of use of advanced technologies.

Replacing human resources with artificial intelligence-based equipment changes the physiognomy of the battlespace. In the same vein, we find a statement by former US Secretary of Defense Mark Esper, who emphasised the importance of artificial intelligence for future conflicts because *"whoever holds supremacy over artificial intelligence will control the battlefield for many, many, many years"*. From this assertion we can conclude that artificial intelligence will illustrate a defining element in holding battlefield supremacy in the context rendered by the decision-action ratio.

We consider it important to bring to the reader's attention, at the end of this chapter, some elements consisting of possible risks caused at the decision-making level, both multi-domain and intra-domain,

by the use of artificial intelligence. Thus, according to the author Sophie-Charlotte Fischer, in the paper entitled *Armament, Arms Control and Artificial Intelligence*, artificial intelligence systems used in the military are still *"fragile and act unpredictably"* (Fischer, 2022, p. 43), with malware attacks being another weakness of these systems. Such shortcomings can also be found in the use of systems that develop artificial intelligence as well as in the escalation – de-escalation conflict ratio, and the consciousness side of the human resource is brought to the fore, which is guided not only by reasoning but also by the sentimental and spiritual side, something that artificial intelligence has not achieved in its evolution and is still in doubt as to whether it will succeed in the future in obtaining this specific human characteristic. The question is whether or not artificial intelligence systems will be able to reach the emotional barrier in the event of a conflict and allow the necessary time to de-escalate the conflict.

AI has managed to achieve a number of results that have surpassed human capabilities, an example being the AlphaGo that managed to beat one of the most titled players worldwide, Lee Sedol.

The ethical issues generated by the use of artificial intelligence (AI) are beginning to become increasingly prominent and justified (Coeckelbergh, 2020, p. 5), issues that are captured in Mark Coeckelbergh's book *AI Ethics* where he examines the current and possible future capabilities of using AI capabilities and the limitations they have compared to the human mind and its rational side. With all these limitations that relate to the rational side, AI has managed to achieve a number of results that have surpassed human capabilities, an example being the AlphaGo that managed to beat one of the most titled players worldwide, Lee Sedol[1] (Borowiec, 2016). The aspect that raises questions from an ethical point of view does not refer to the way AlphaGo managed to defeat Lee Sedol, but to the reaction he had to his defeat, which shows emotional involvement as a result of human consciousness and feelings compared to his *"opponent"* that does not emit such human characteristic feelings. The examples given here, which relate to the ethics of using artificial intelligence, are intended to highlight the importance of the way in which new technologies are used and the fact that an evasive approach to issues relating to the typically human emotional side can have negative effects on the *human resource-artificial intelligence* collaborative framework.

[1] Lee Sedol, South Korean professional *Go* player.

Artificial intelligence, as an element that marks human existence, must be fully accepted because the future will increasingly expose us as a society to technology and digitalisation, and intelligent systems will be more and more part of human life, regardless of our will because, as we have mentioned throughout the article, man has an evolutionary tendency already demonstrated by the space-time spectrum.

CONCLUSIONS

The implementation of the multi-domain operations concept in all North Atlantic Alliance member states will probably become a necessity and a standard to be achieved by all of them, in all military services, in order to further strengthen the idea of common defence. The national documents of countries that have not taken visible steps in this direction will have to align themselves with Alliance requirements and, at the same time, adapt their internal structures to the conditions that the implementation of this concept imposes on their infrastructure and capabilities. These actions foresee, in particular, the involvement of strategic level command points, consisting of a joint effort with national and international implications on the development of capabilities operating on the basis of advanced technologies, the goal of which may be to generate cross-domain operability.

The doctrinal and strategic mainstreaming of the concept of Multi-Domain Operations provides a unified view of the North Atlantic Alliance and also fosters and facilitates a common vision of how Member States should systematise their working methods to conduct actions in a multinational framework and to create a suitable environment for operationalising the concept.

The doctrinal and strategic mainstreaming of the concept of Multi-Domain Operations provides a unified view of the North Atlantic Alliance and also fosters and facilitates a common vision of how Member States should systematise their working methods to conduct actions in a multinational framework and to create a suitable environment for operationalising the concept.

We believe that the corresponding processes of decision-making and, respectively, the concretization of decisions in action are key elements that emerging and disruptive technologies must augment, by fully or partially supplanting the work of human resources, so that the operationalisation of the concept can acquire an integral form through the maximum use of these resources. Although artificial intelligence is useful in the conduct of military operations and actions, in the context of ISR (intelligence, surveillance, reconnaissance) missions, its potential is certainly much more advanced.

The non-military sphere that foresees applications of artificial intelligence in the functioning rhythm of society, as mentioned throughout this article, faces situations that concern ethics and its derivates when the human resource is replaced. The military system, with the integration and development of military intelligence within its own structures and at various stages of the military operation process, may face difficulties in using these technologies to the extent that they can assume independent decision-making powers in the battlespace. Elementary characteristics of the human being, such as rationality or consciousness, will be elements that may be difficult to attribute to systems based on artificial intelligence, hence the issue of ethics and the main difference at this point between the human factor and this type of emerging technology, concluding that the decision at any level must still be taken by the human being.

The future perspective on how to integrate the concept of Multi-Domain Operations at the doctrinal level captures emerging and disruptive technologies as key elements that will underpin the operationalisation process itself, ultimately providing the practicality of this broad concept, which is that, at the architectural level, the battlespace infrastructure will be rendered by the ability to interconnect technological capabilities.

The concept of multi-domain operations will be a standard according to which the North Atlantic Alliance and its member states will have to adapt and organise their security and defence systems through the integration and use of advanced technologies.

Also, the integration of the two new domains, space and cyber, into the operational sphere is a result of advanced technologies or, in other words, has been imposed by technological development. In the absence of existing capabilities, it would probably be difficult to project a clear picture of cyber warfare, for example, as there is still an anticipatory level based on theoretical segments, an idea that would also be true for multi-domain operations. The concept of multi-domain operations will be a standard according to which the North Atlantic Alliance and its member states will have to adapt and organise their security and defence systems through the integration and use of advanced technologies.

In conclusion, we can add that the generation of an environment in which society will be under the spectrum of security and protection is based on concrete actions that are low risk and where emerging and disruptive technologies can become essential pillars to achieve this goal.

BIBLIOGRAPHY:

1. Architecture Working Group (18 December 1997). *C4ISR Architecture Framework Version 2.0*.
2. Borowiec, S. (15 March 2016). *AlphaGo Seals 4–1 Victory Over Go Grandmaster Lee Sedol, Guardian,* https://www.theguardian.com/technology/2016/mar/15/googles-alphago-seals-4-1-victory-over-grandmaster-lee -sedol, retrieved on 3 February 2024.
3. Chairman of the Joint Chiefs of Staff (8 June 2018). *Cyberspace Operations*, https://irp.fas.org/doddir/dod/jp3_12.pdf, retrieved on 2 February 2023.
4. Coeckelbergh, M. (2020). *AI ETHICS*. London: The MIT Press.
5. Davis, Z.S. (March 2019). *Artificial intelligence on the battlefield*. Center for Global Security Research. Lawrence Livermore National Laboratory.
6. Fedasiuk, R., Melot, J., Murphy, B. (October 2021). *Harnessed Lightning*. Center for Security and Emerging Technology, https://cset.georgetown.edu/wp-content/uploads/CSET-Harnessed-Lightning.pdf, retrieved on 1 February 2024.
7. Iancu, N. (29 July 2019). *Noul dicționar al apărării: tehnologiile disruptive*. Monitorul Apărării și Securității, https://monitorulapararii.ro/noul-dictionar-al-apararii-tehnologiile-disruptive-1-21024, retrieved on 31 January 2024.
8. Johnson, J. (2023). *AI and the Bom – Nuclear Strategy and Risk in the Digital Age.* New York: Oxford University Press.
9. Kania, E.B., Costello, J.K. (12 September 2018). *Quantum hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership*. Center for New American Security, https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Quantum-Tech_FINAL.pdf?mtime=20180912133406, retrieved on 3 February 2024.
10. Miller, R., Enda, C. (25 January 2024). *US Extends Lead Over China in Race for World's Biggest Economy*. Bloomberg, https://www.bloomberg.com/news/articles/2024-01-25/us-extends-lead-over-china-in-race-for-world-s-biggest-economy?leadSource=uverify%20wall, retrieved on 3 February 2024.
11. Ministerul Apărării Naționale/Ministry of National Defence (2021). *Strategia Militară a României/Military Strategy of Romania*. București.
12. Ministry of Defence (2020). *Multi-Domain Integration*. United Kingdom.
13. NATO (December 2022). *Allied Joint Doctrine*.
14. Perkins, W.A. (2018). *Component Integration Challenges presented by Advanced Layered Defence Systems (A2/AD),* in The Three Swords Magazine.
15. Perry, W., Signori, D., Boon, J. (2004). *Exploring information superiority*. Santa Monica: RAND Corporation.
16. *Prezentatorii de știri TV, înlocuiți cu roboți umanoizi autonomi pe baza de A.I. în China*, https://www.gadget-talk.ro/roboti-umanoizi-autonomi-prezinta-stiri-china/, retrieved on 29 January 2024.
17. Reinhold, T., Schörnig, N. (2022). *Armament, Arms Control and Artificial Intelligence.* Cham: Springer.
18. Ross, R., Pillitteri, V. (December 2021). *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. National Institute of Standards and Technology – US Department of Commerce.
19. The United States Army War College (2020). *Mission Command of Multi-Domain Operations*.
20. UN News (6 July 2023). *Meet the robots who are making the world a better place*, 6 July 2023. Africa Renewal, https://www.un.org/africarenewal/magazine/july-2023/meet-robots-who-are-making-world-better-place, retrieved on 29 January 2024.
21. US Army (7 July 2020). *Army Futures Command Concept for Maneuver in Multi-Domain Operations 2028*.
22. Wade, N.M. (2020). *The Battle Staff SMARTbook*. The Lightning Press.

ROMANIAN MILITARY THINKING

THE DIGITALIZATION OF CRITICAL INFRASTRUCTURES – SYSTEMIC CONSIDERATIONS, EVOLUTIONS OF GOVERNANCE AND ELEMENTS OF A NATIONAL RESEARCH AGENDA –

Adrian Victor VEVERA, BEng, PhD
General Director, National Institute for Research and Development in Informatics-ICI, Bucharest
10.55535/RMT.2024.3.6

The rapid digitalization of all aspects of economic, social, and political life in advanced societies has produced new risks, vulnerabilities, and threats. Rapid technological change is generating new systemic trends related to digitalization. This article presents the main arguments in favour of this view and attempts to delineate the main transformations that will take place, while emphasizing their impact on societal security, including at the level of defence. It does so through the critical infrastructure protection framework, which provides a system-of-systems perspective uniquely suited to the analysis of complex systems and processes.

Keywords: digitalization; resilience; critical infrastructures; emerging technologies; system-of-systems;

INTRODUCTION

Digitalization is a quantitative and qualitative process through which digital technology becomes embedded into key social, economic, and political processes[1]. Based on the revolution in connectivity and computing power, whereby more data transfer capacity and more computing power are made available at lower prices to greater numbers of users, digitalization has changed the face of all societies, including developing ones. This article presents a transversal analysis of the cyber domain using the framework of Critical Infrastructure Protection (CIP). Utilizing this framework provides us with key concepts and terminologies to use a system-of-systems approach in analysing the systemic impact of digitalization, the changes in the cybersecurity environment, and the changes in governance processes. The article ends with a non-exhaustive list of recommendations for priority research and development areas for Romania.

CIs criticality stems from the fact that, according to legislated methodologies for identification and designation of CIs, their disruption or destruction would cause significant loss of human life, material damage and loss of confidence on the part of citizens, investors, partners and allies, among other effects.

DIGITALIZATION AND CIP THEORY

CIP theory relies on the concept of Critical Infrastructures (CI), which are socio-technical systems made up of assets, resources, components, and organizations working together to produce critical goods and services. Their criticality stems from the fact that, according to legislated methodologies for identification and designation of CIs, their disruption or destruction would cause significant loss of human life, material damage and loss of confidence on the part of citizens, investors, partners and allies, among other effects. CIP enables us to develop a systemic view of the functioning of advanced societies, both internally and cross-border, or even at global levels, in order to manage the risks, vulnerabilities and threats that global infrastructure connectivity,

[1] Note: This article summarizes the main theoretical conclusions of the book *A Transversal Analysis of the Cyber Domain in Critical Infrastructure Protection*, Vevera, A-V (2022). București: Editura Militară.

natural disasters and deliberate actions on the part of malignant or criminal actors have generated. CIs are often interdependent, whereby changes in one infrastructure generate changes in another, based on a geographical, logical, physical, or informational relationship. Thus, they are often affected by disruptions stemming from common causes, which lead to aggravated and prolonged crises, and they can even experience cascading disruptions, where a chain of interdependent infrastructures is disrupted in sequence. (Bucovețchi, Simion, 2015).

Digitalization is a leading factor in the greater coordination and integration of critical infrastructure, beyond national borders and even at global level. Digital systems provide command, control, coordination, and data gathering capabilities that enable the safe and predictable operation of critical infrastructures across vast geographic distances, requiring various components, which are sometimes infrastructures in themselves, to work in unison to achieve productivity, reliability, affordability and safety.

Digitalization is a leading factor in the greater coordination and integration of critical infrastructure, beyond national borders and even at global level. Digital systems provide command, control, coordination, and data gathering capabilities that enable the safe and predictable operation of critical infrastructures across vast geographic distances, requiring various components, which are sometimes infrastructures in themselves, to work in unison to achieve productivity, reliability, affordability and safety. For CIs, digitalization does not mean just communication and databases, as it does for most users, but also the emergence of cyber-physical systems that rely on digital mechanisms to interpret signals from the physical world and to give commands to systems, which create an effect in the physical world. The industrial control systems (ICS) as well as supervisory control and data acquisition systems (SCADA), which have become central to the operation of many CIs across different sectors, are all the result of digitalization and networking.

Thus, critical infrastructures are exposed to various risks and threats, such as those posed by hackers. At the same time, decision-makers and policymakers in the field of security governance have to protect these systems and increase their resilience, which is their capacity to prevent an accident or thwart attacks and, if they happen anyway, to minimize damage and disruption times and to resume as soon as possible a minimum acceptable level of functioning, while extracting lessons learned. However, the rapid advances in digital technology and the continuing rise of digitalization are changing key paradigms, and stakeholders must rapidly adapt to the new security environment and the new evolution of the critical infrastructures.

SYSTEMIC TRANSFORMATIONS IN THE CYBER FIELD

The phenomenon of digitalization has led to obvious changes in how we work, shop, educate ourselves or interact. For better or worse, they are reshaping human relationships and societies. This is a systemic effect. When seen from a Critical Infrastructure Protection framework, digitalization also has a systemic effect and it, too, has both positive and negative effects.

We are undergoing a process of acceding to a new paradigm of digitalization, characterized by the following features:

- It is based on ubiquitous computing and connectivity between system components;
- There will be no more dumb or non-networked systems, except by intentional design and at the cost of efficiency and usability;
- It is integrating new technologies, especially emerging technologies such as AI, blockchain, quantum computing;
- It is generating new risks, vulnerabilities and threats, as well as accentuating the lack of predictability of the resulting system and the mismatch between the systems whose security needs to be governed and the governance system, which is based on territorialized understandings of jurisdiction and action.

The negative consequences of new technologies and the patterns of interaction and activity they generate can be profound. The most visible examples are those resulting from deliberate human action, for manipulative, disruptive or destructive purposes, both for profit (organized crime) and for political, social, and ideological purposes (cyber terrorism, hacktivism etc.).

The negative consequences of new technologies and the patterns of interaction and activity they generate can be profound. The most visible examples are those resulting from deliberate human action, for manipulative, disruptive or destructive purposes, both for profit (organized crime) and for political, social, and ideological purposes (cyber terrorism, hacktivism etc.).

There are significant categories of consequences that do not come from human deliberation or decision, but result from the interaction between various systems, sub-systems, and their environment, which generates unpredictable, emergent, and uncertain effects, phenomena and behaviours. The intersection of natural phenomena and deliberate threats produces new patterns of disruption or degradation of CI. It affects not just cyber infrastructure, but every CI that relies on digital systems for command, control, and coordination.

We can identify four main systemic transformations.

The Revolution of Scope and Scale

Digitalization revolutionizes the scope and the scale of critical infrastructures acting within a wider system-of-systems by enabling better control and coordination among large or dispersed assets or within production and supply chains. This phenomenon has been taking place ever since the revolution in communications represented by the telegraph. The digital and connectivity era has enabled higher volumes of information and greater automation in systems, which has made CI systems-of-systems truly global not just in their impact, but also in their degree of control and coordination. *Figure 1* shows the degree to which EU Member States have digitalized, expressed through the *Digital Economy and Society Index.*

Digitalization revolutionizes the scope and the scale of critical infrastructures acting within a wider system-of-systems by enabling better control and coordination among large or dispersed assets or within production and supply chains.

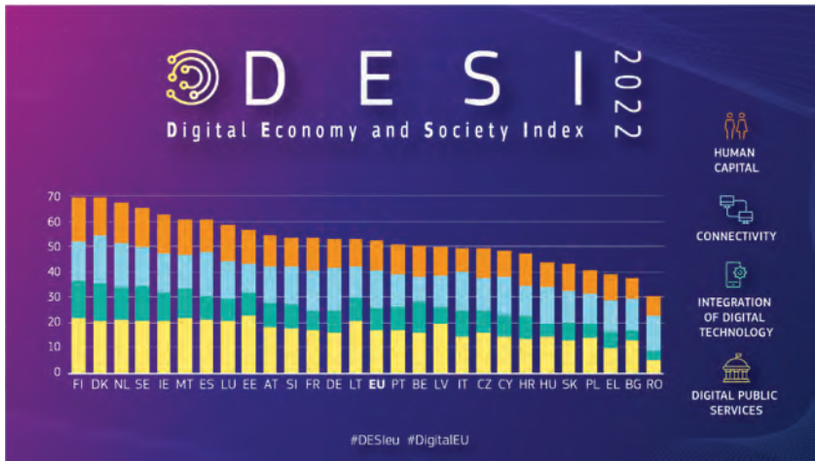


Figure 1: Digital Economy and Society Index 2022
(European Commission, 2023, https://digital-strategy.ec.europa.eu/en/policies/desi)

The Transition from Proprietary Systems to Commercial-Off-The-Shelf (COTS) Systems

Many of the most sensitive and function specific critical infrastructures require specific assets, hardware and software, in order to operate. Their initial digitalization in the form of industrial control systems was done through bespoke hardware and software, developed internally or tailor-made by an external contractor, often working in obscure programming languages. Gradually, the growth of digitalization created a digital mass of services and other capabilities which could be adaptable to various needs in order to provide the scale required for economic efficiency and high investment in research and development. Concentration effects in technological ecosystems, where a series of solutions and standards could win over others, also took place. What that means is that Critical Entities or Critical Infrastructure Operators no longer need bespoke systems and are actually better off not trying to develop them. They can buy hardware and software from the mass market, at better prices, with better performance, with better lifetime cost and upgrades and with better security in other ways, including time for repairs and maintenance, vulnerability to various hazards and so on. Even if an entity develops a bespoke system, that system will likely still use some components, such as sensors, coming from specialized producers, which supply the rest of the market, or software that uses open-source libraries or a particular operating system. Their own vendors are also dependent on commercial supply chains and are themselves suppliers for a wider array of actors. (Nazir et al., 2017; Mehta, Reddy, 2015). It translates into a reduction in security through obscurity, the quality of being harder to hack or disrupt because most potential attackers lack specific knowledge about your systems, your programming language, your software etc. Most attackers of such systems are either highly specialized entities with state backing or internal threat actors. On the other end of the scale, the emerging paradigm sees CI operators relying on complex systems made up of commercial-off-the-shelf hardware, software, public communication links (the Internet) and other generic solutions. We are not just discussing Enterprise Resource Management solutions such as SAP or office software suites for organizations, but also the industrial control systems themselves. It means that a hacker can use the same set of general knowledge to effectively attack (though maybe not with ideal performance as that given by specific knowledge) any system, whether it is a thermal power plant, a data centre, a waste treatment facility, a logistics company, or a large retailer.

The growth of digitalization created a digital mass of services and other capabilities which could be adaptable to various needs in order to provide the scale required for economic efficiency and high investment in research and development. Concentration effects in technological ecosystems, where a series of solutions and standards could win over others, also took place.

The process is still ongoing, with new horizons for COTS paradigms, such as satellites running on Android mobile operating software, or facilities retooled under an Internet-of-Things paradigm, full of wireless

sensors and access nodes, including for non-essential functions such as office lights, centralized heating-ventilation-air-conditioning systems and other systems that are unpatched or unpatchable across the product lifetime and can provide access points into company networks for enterprising hackers. That is is also why supply chain attacks have grown so much in recent years, as well as attacks through unreported backdoors, vulnerabilities and zero-day exploits.

Infrastructure Reorganization

Digitalization is enabling the reorganization of critical infrastructures to take advantage of the new possibilities offered by connectivity, computing, high levels of data transfers and automation. This reorganization can take place at physical level, at cyber level, at economic level and at organizational level, and can result in new infrastructure typologies that generate new risks, vulnerabilities and threats.

Digitalization is enabling the reorganization of critical infrastructures to take advantage of the new possibilities offered by connectivity, computing, high levels of data transfers and automation. This reorganization can take place at physical level, at cyber level, at economic level and at organizational level, and can result in new infrastructure typologies that generate new risks, vulnerabilities and threats. The process is ongoing, because of the gradual nature of digitalization and the adoption of new technologies, which depend not just on technological levels, but also on economic incentives such as competition, on capital expenditure requirements, on appetite for risk and on general market evolution.

The best example of a strong reorganization effect has been the trend in recent decades for production offshoring and outsourcing, which has led to globally fragmented production and supply chains kept functioning by just-in-time logistical systems first pioneered by Japanese companies. It enabled entities to move production where labour and other input costs were lower. It resulted in decentralized production chains, even within the same company, requiring global coordination mechanisms that were managed digitally. The security costs of that model were seen in the growing exposure to cyber attacks, but also in supply issues when events like conflicts or the 2020 pandemic interrupted cross-border transport.

A more recent example of reorganization is the rise of cloud computing, whereby distributed computing systems (each worker with own desktop, laptop, with processor, memory, or each company with its own servers) were replaced by work stations that depended

on centralized computing and memory. It enabled lower costs, more rapid scaling of services for growth, more flexible allocation of resources (you pay for the computing power used without capital expenditure in your own systems), easier upgrade and replacement and better security (since systems could be professionally run, administered or replaced). However, it is creating a single point of failure for the entire enterprise (in the case of a dedicated company cloud) or for an entire ecosystem of entities relying on a very big cloud services provider (the marketing being concentrated among three great actors – Microsoft, Google, Amazon). Even when trying to avoid this development, many services that are used by an entity might have cloud processes running in the background, so there is an indirect risk.

Extreme examples of reorganization have led industrial aerospace giants like Boeing or tech giants like Apple to become technology integrators, performing research and handling marketing, finance and other functions, while outsourcing and offshoring most the actual production chain to other actors.

Infrastructure Virtualization

One particular form of reorganization of CI is the virtualization of the CI, in which critical elements of differentiation between specific CI processes are moved from the physical space into the virtual one, where it becomes very difficult to delineate between one process or another and between one infrastructure or another, especially when it comes to cyber infrastructures or their components.

One particular form of reorganization of CI is the virtualization of the CI, in which critical elements of differentiation between specific CI processes are moved from the physical space into the virtual one, where it becomes very difficult to delineate between one process or another and between one infrastructure or another, especially when it comes to cyber infrastructures or their components. We can no longer pinpoint a particular physical asset involved in a process. It has numerous implications for various aspects of CI functioning, such as single point failures, common cause failures, escalating failures, cascading failures and more. The consequences are profound, from a security governance perspective, since it makes CI much more malleable and therefore harder to adequately map, interpret, explain and predict. Key processes are transformed into specific software running on generic hardware which is delocalized. The previously mentioned cloud infrastructure is one such example, but we may also include here various elements of the 5G communications infrastructure,

which is what raised the spectrum of security issues related to the Chinese vendor ecosystem for 5G solutions, since core and periphery elements of the 5G infrastructure could no longer be separated to reduce security risks. A simple example is a company or a department inside a company providing critical coordination services for industrial manufacturing processes, for market operations or for logistics. Once, it would have had its own data centre with physicalized infrastructure that it could shut off, physically disconnect, replace or segment. Then, it started leasing this infrastructure from a particular company, which provided it with its own dedicated facility or sector of a facility. Afterwards, the solution vendor moved the company's processes onto much larger and more efficient servers, which it segmented virtually into dedicated space or *"devices"* for that company's operation. Lastly, the infrastructure became completely virtualized, running on a virtual infrastructure made up of hundreds of data centres, being everywhere and nowhere all at once so that no amount of maintenance or power outages would require planning the continuity of service, given that the infrastructure reorients itself automatically around non-functioning elements. It has great advantages from a cost and safety perspective, but also increases the risks associated with a successful cyber attack or another phenomenon (electromagnetic pulse) targeting the infrastructure itself.

The virtualization of infrastructure leads to new paradigm shifts, such as: IaaS – Infrastructure as a Service; SaaS – Software as a Service; PaaS – Platform as a Service.

The client has very little say over the day-to-day management of that infrastructure – its maintenance cycles, its communication technology, its upgrades, its cybersecurity measures etc.

The virtualization of infrastructure leads to new paradigm shifts, such as:

- IaaS – Infrastructure as a Service – in which a competing cloud provider offers distributed computing services;
- SaaS – Software as a Service – in which cloud computing is used for software distribution;
- PaaS – Platform as a Service – where the cloud computing provider provides the platform for building new applications by developers, who then find customers for a specific service running on a generic platform.

Blockchain technology enables an even greater decentralization and unbundling of critical organizational functions for critical infrastructures. The ability to have smart contracts run automatically rather than depend on a third party such as a bank or a dedicated department for assurance will lead to even more virtualized infrastructures.

Blockchain technology enables an even greater decentralization and unbundling of critical organizational functions for critical infrastructures.

EVOLUTION OF THE CYBERSECURITY ENVIRONMENT

The cybersecurity environment is undergoing rapid change due to technological development and a greater permeation of economic, social and political life, especially after the smartphone revolution. While certain aspects of this change are unknowable, given the uncertainties regarding rates of technological adoption and the speed of new breakthroughs, we can safely assume that the cybersecurity environment is dynamic, multifaceted and challenging. A thorough analysis of the scientific literature and especially the industry reports that keep track of the changing security priorities can let us aggregate various information into a series of key trends, summarized in *table 1.*

Table 1: Trends in the cybersecurity environment (Vevera, 2022)

Trend	Explanation
Increased surface area for contact	Various technological and economic trends have increased the contact surface between the real world and the cyber world, as well as between the systems that need to be secured and a chaotic and dangerous cyber security environment. The contact surface metaphor expresses the increase in deliberate as well as accidental interactions, and the proliferation of attack opportunities, especially through the exploitation of unknown vulnerabilities and access paths by defenders.

Trend	Explanation
The variety of actors involved	The actors who deliberately attack critical infrastructures are varied and changing. Among them, we list: • Cross-border criminal organizations; • Lone wolves; • Non-state groups driven by ideology; • Rebellious states (rogue); • Groups sponsored by states; • The enemy within the organization; • Combinations of them.
The complexity of motivations	Some actors seek profit, others wish to apply coercive measures to change the behaviour of the state or targeted actors, and others act out of ideology. Frozen conflicts between states are another contributor to such motivations. It should be noted, however, that many actors have mixed motivations, and a trend noted by O'Gorman et al. (2019) refers to the increasing profit motivations of state-supported actors.
The commodification of malware	The traditional model is one where the attacker develops its own means of attack and the skills to use them, which naturally limits the number of attackers and attacks. Today, however, especially through the anonymity promoted by cryptocurrencies, malware has been commodified so that malware production and even its use can be outsourced. An aspiring attacker can buy a particular application and use it to accomplish their goals with a tool that is likely much better than what they could have developed on their own. The proliferation of cyber weapons following their loss by intelligence agencies contributes to this phenomenon.

The cybersecurity environment is undergoing rapid change due to technological development and a greater permeation of economic, social and political life, especially after the smartphone revolution.

Trend	Explanation
Cyber criminals are mirroring legitimate business practices	The trend was noted by Fortinet (2013), being a development of the phenomenon detailed before. Developed markets are emerging to facilitate the division of labour in cyber attacks. Bidders adopt legitimate business techniques and compete with each other to attract customers. A customer may purchase specific malware or information related to vulnerabilities; can rent virtual machines and computers with pre-existing malware infections for a DDoS attack; can acquire passwords and bank data in large quantities, hoping to be able to embezzle funds and so on.
Unequal rates of advancement	The cyberspace is advancing faster than the security culture of users or the governance capacity of authorities and large companies, which increases the opportunities for enterprising criminals.
The link between cybercrime and cyberterrorism	Terrorism and cross-border organized crime are closely linked. First, the terrorist is often a cybercriminal himself in order to finance himself, obtain information about the target, and coordinate with other entities. Second, organized crime provides a market for goods and services for terrorists – cyber weapons and the ability to purchase specific services, including information and vulnerabilities, but also the destructive effect that organized crime and corruption have on targeted organizations.
Technological evolution	The emergence of blockchain-based ransomware and, more recently, the replacement of Trojan worms with ransomware as contagious malware. The field is dynamic and innovative, where new ideas spread quickly and are reflected in the level of new threats.

ROMANIAN MILITARY THINKING

The cyberspace is advancing faster than the security culture of users or the governance capacity of authorities and large companies, which increases the opportunities for enterprising criminals.

Trend	Explanation
Systemic fragility	Field-wide technological developments have encouraged systemic changes, some detailed in the previous section, that have increased the vulnerability of critical infrastructures to accidental and deliberate threats. There are many more opportunities to disrupt the good functioning of a system, and systemic transformations have reduced system-wide resilience, robustness, adaptability, redundancy and other attributes of resilience.

The cybersecurity environment is registering an increase in malignant activities due to a lack of a proper global cybersecurity architecture and framework, coupled with the high potential gains, both financial and strategic, from engaging in such activities.

We can be quite certain that the cybersecurity environment is registering an increase in malignant activities due to a lack of a proper global cybersecurity architecture and framework, coupled with the high potential gains, both financial and strategic, from engaging in such activities. In line with the increase in the surface contact area between critical infrastructures, the Internet and networked systems in general, we can assert that the frequency and severity of attacks and infiltrations are growing. Because of the cyber-physical system paradigm, the cyber attacks are also having more and more impact in the physical world, especially when it comes to critical goods and services or the critical coordination necessary for avoiding disastrous effects in the physical world from disturbances in the functioning parameters of critical infrastructures.

TRANSVERSAL APPROACHES

We have picked two transversal approaches to the issue of digitalization seen through a CIP lens. The first is the analysis of the European framework for cyber issues, seen in a wider sense, encompassing both legislation and institutions. The second is sketching a national agenda for targeted developments in cyber issues in order to deal with the impact of digitalization.

The European Framework for Handling Systemic Digitalization

Starting with the first Green Book on Critical Infrastructure Protection in 2004 and reaching fruition with Directive 114/2008 on the Identification and Designation of Critical Infrastructures, the European Union has developed a comprehensive framework for CIP under the European Programme for Critical Infrastructure Protection (EPCIP). The Programme differs from the US version through the politically necessary distinction between the EU and Member States, entailing a distinction between national CIs and European CIs. Member States are responsible for both, but EPCIP has a special role in administering European CIs, whose disruption or destruction would affect two or more Member States. Under the latest EU Critical Infrastructure Blueprint, a new category of ECIs has been defined, affecting six or more Member States. This stronger form of subsidiarity is a political necessity and creates important challenges, which the multilateral framework strives to overcome.

Starting with the first Green Book on Critical Infrastructure Protection in 2004 and reaching fruition with Directive 114/2008 on the Identification and Designation of Critical Infrastructures, the European Union has developed a comprehensive framework for CIP under the European Programme for Critical Infrastructure Protection.

Cyber is an important part of EPCIP and associated efforts, and the European governance regime for systemic issues has been enhanced over time with a *European Cybersecurity Strategy*, the *Network and Information Security Directive (NIS)* and a host of other documents of reference. The governance regime has both legislative and institutional components. *Figure 2* represents an attempt to map the institutionalized European framework for cybersecurity, both legislatively, strategically, operationally, and from a research and innovation perspective.

From a legislative perspective, we have chosen to highlight a particularly important recent development – the 2023 political approval of the *Critical Entities Resilience Directive (CER)* and the *NIS 2 Directive*, with planned transposal into Member State legislation by October 2024, though it seems optimistic, given the breadth of changes they introduce.

The two Directives maintain continuity with EPCIP, but introduce major systemic changes that are the result of the lessons learned from the pandemic and from the war in Ukraine, in terms of the true interconnectivity between the CIs of Member States at European level, both within sectors and across different sectors. The most important feature from the perspective of our analysis is that the cyber

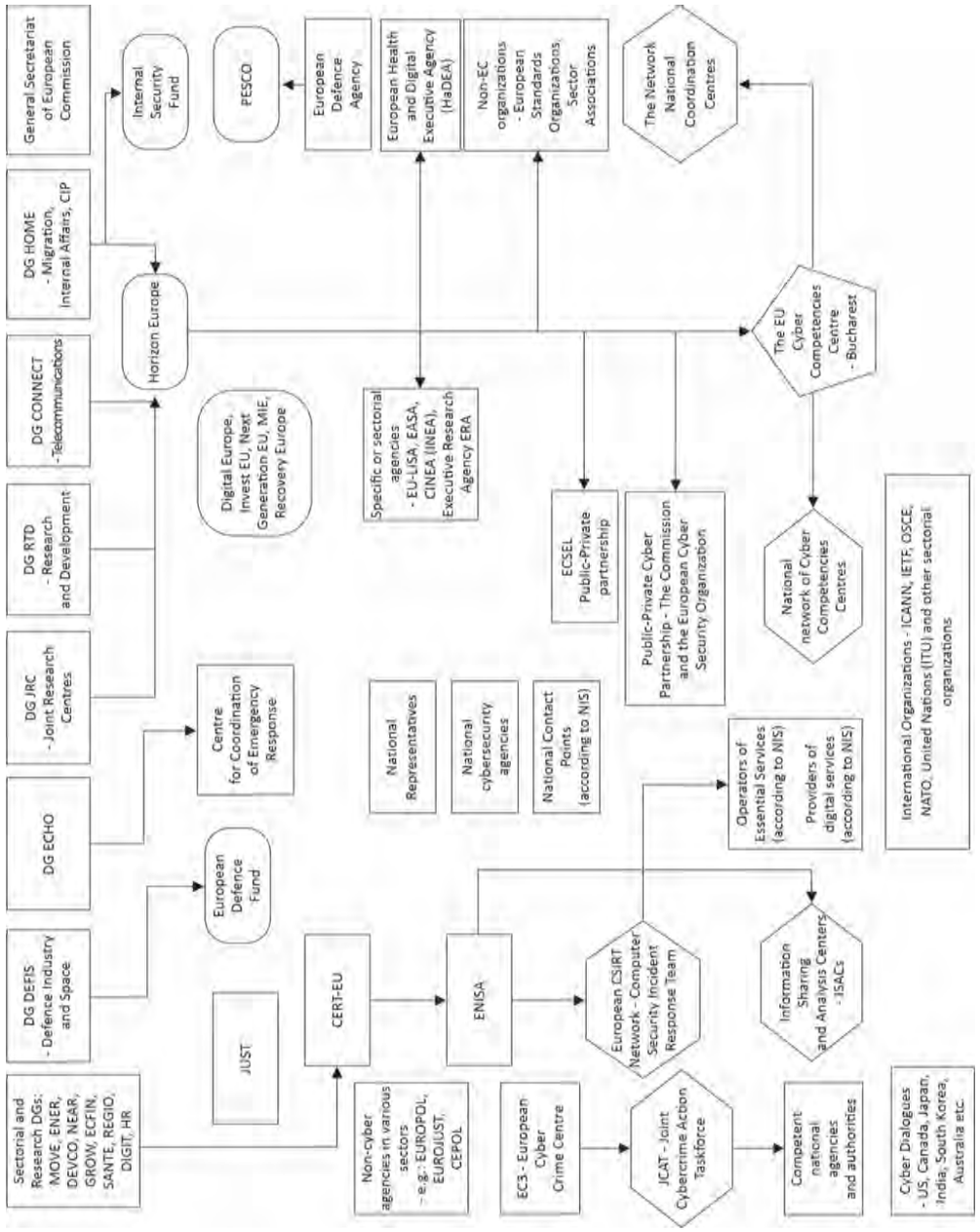


Figure 2: Map of European cybersecurity governance (Ib.)

dimension now permeates all the CIP governance framework, through the fact that the taxonomies of essential/critical/important systems identified by the two Directives now overlap almost completely. Every CI in the CER Directive is also present in the NIS 2 Directive, while the NIS 2 Directive also creates an additional category for less than critical systems such as postal services. *Figure 3* presents this overlap.

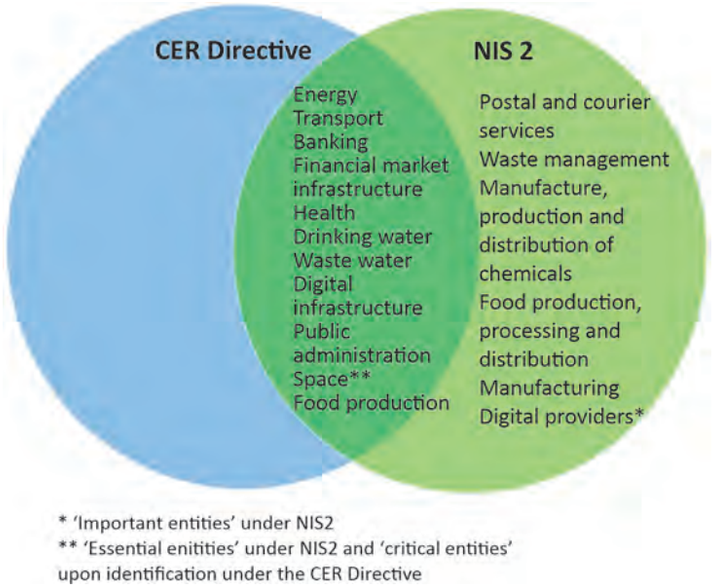


Figure 3: Overlap between CER Directive and NIS 2 (Georgescu, Bucovețchi, 2023)

The cyber dimension now permeates all the CIP governance framework, through the fact that the taxonomies of essential/critical/important systems identified by the two Directives now overlap almost completely.

We see the following main changes:

- The adoption of the term *"entity"* from the NIS methodology as the building block of EPCIP efforts, replacing almost entirely the concept of critical infrastructure *owner/operator/administrator*. It leads to a more expansive definition of CIs, which also encompasses aspects related to the organization that owns and runs it, including also financial and ownership dimensions;
- The addition of nine new European CI sectors, after energy and transport, which were already in EPCIP. The new 11 sectors are energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, food, digital infrastructure,

public administration, and space. It was mainly the result of the recorded impact of the pandemic, but a tendency towards expansion had already been noted through European framework developments on cyber and through European projects on critical space infrastructures supplying critical services requiring dedicated European agencies to manage;

- A more developed European methodology to assist in the identification and designation of critical entities;
- Lower thresholds for criticality, meaning that more critical entities will be identified and designated compared to the previous models, which underestimated the required size and scope for a critical infrastructure to have systemic effects in case of its disruption;
- The development of a new category of critical entity (the critical entity of special importance), which affects a third or more Member States and which requires special coordination and resources to protect, increase its resilience and recover from disruptions. They also require stronger mechanisms for identification and designation through a collective approach;
- The development of a Critical Entities Resilience Group, made up of Commission experts who assist Member States and national authorities in the various EPCIP processes;
- The development of new networks and institutions/agencies, such as Cyber Competencies Centres and Information Sharing and Analysis Centres (ISACs) at European and national levels, constituting important networks for multilateral governance.

The national security and defence of Romania in the context of rapid digitalization of its own infrastructures and systems, as well as those of commercial partners, security partners and allies, require a proactive approach to the development of a cyber-resilient society.

Towards a New Agenda for Romanian Responses to Systemic Digitalization

The national security and defence of Romania in the context of rapid digitalization of its own infrastructures and systems, as well as those of commercial partners, security partners and allies, require a proactive approach to the development of a cyber-resilient society.

Table 2 identifies key priorities for research and development for Romanian private and public actors. This is not an exhaustive list, but one that covers a large spectrum of systemic cyber threats, including emerging technologies, new architectures and strategic priorities.

(Vevera, Cârnu, Rădulescu, 2022). It is not feasible for the Romanian technological ecosystem to develop all of them on its own to adequate levels. Therefore, Romanian security consumers need to be aware of the threats to identify supply chains and vendors that can provide solutions when they are needed, whether they come from Romanian entities, Romanian subsidiaries of foreign companies or foreign companies headquartered in allied states with secure supply chains.

Table 2: Priorities for cyber research to address systemic issues (Vevera, 2022)

Priority	Explanation
Integrating AI technology into remote authentication systems	AI technology can be used to introduce an additional level of security against the backdrop of the increase in remote working, through digital means, encouraged by the Covid-19 pandemic.
Researching digital forensic methods on Deepfake media content	Deepfakes are a type of synthetic media content where the behaviour of a person in an existing video is intentionally altered. It is used in disinformation and other hybrid operations. The emergence of these new digital means of manipulation generates the need and the opportunity to create innovative products to address the problem.
Analysis of the security and integrity of smart contracts used in Blockchain technology	Smart contracts allow the execution of credible transactions without the involvement of third parties to validate them. These transactions are public and irreversible in blockchain technology. The integration of blockchain applications not only in the area of cryptocurrencies, but as part of the background processes in the functioning of financial, logistical and administrative operations generates opportunities to create new products with security impact, but also the need to ensure security against terrorism, money laundering and attempts to manipulate and interrupt these processes.
Design and analysis of the architecture of self-sovereign digital identity systems (SSI)	SSI deals with the problem of establishing trust in an interaction. To be trusted, one party to an interaction will present its credentials to the other parties, and those parties can verify that the credentials come from an issuer they trust. In this way, the trust of the verifier in the issuer is transferred to the holder of the accreditation. These systems require new system architectures and innovative encryption solutions.

Deepfakes are a type of synthetic media content where the behaviour of a person in an existing video is intentionally altered.

Priority	Explanation
Research of adaptive networks based on analytical and business data	Adaptive networking is a new approach that expands on autonomous networking concepts to transform the static network into a dynamic, programmable environment driven by data analytics and intelligence. There are also applications for AI, going as far as autonomous decision-making systems, with security impact, as well as generation of new capabilities, including in the field of security.
Researching cyber threat detection methods using supercomputing (HPC) technology	HPC generally refers to the practice of aggregating computing power in a way that provides much higher performance than could be obtained from a desktop or workstation computer to solve problems of high complexity. The use of these applications, in conjunction with AI and other tools and capabilities, will respond to the need to ensure resilience in the face of a challenging security environment, with diverse and ubiquitous threats that require increased reaction capacity and new capabilities to analyse, attribute, limit effects and prevent intrusions.
Researching post-quantum cryptography methods	Quantum computing promises, once it becomes commercially available, to render existing encryption technologies obsolete. Therefore, there is a race to explore quantum-secure encryption methods, which can theoretically provide data security, and quantum-safe encryption methods, which can provide absolute certainty that they cannot be decrypted. Many research institutes are working on it, with the NIST in the US having already proposed 60+ quantum-secure methods of encryption, but some of them have already been broken. Therefore, this is an ongoing concern.
The transition of traditional network infrastructures to Zero-Trust architecture	A zero-trust security model requires that every device in a network undergoes a strict identity check every time it authenticates to the network, regardless of its location (whether it is inside the network or outside the network perimeter).

Quantum computing promises, once it becomes commercially available, to render existing encryption technologies obsolete.

Priority	Explanation
Cyber security research and the use of AI in addressing the problems of aggression and warfare in the electromagnetic spectrum	The anticipated revolution in the field of 5G, the ubiquity of mobile communications by various means (including Wi-Fi networks) and the implementation of wireless communication systems between the components of critical infrastructure systems such as sensors (even between the components of compact systems such as satellites), or in the framework of some distributed weapons systems generates a new security environment, exposed to attempts at jamming, signal hacking and data theft. As part of the hybrid war, we anticipate the evolution of electronic warfare as a means of diminishing the military capabilities as well as the civil infrastructures functioning. At the same time, we can anticipate the use of means of electronic warfare supported by AI decision-making systems related, for example, to signal modulation, as a means of equalizing military capabilities in the face of stronger and better equipped adversaries.
Using AI technology for new weapon systems	AI technology can be used for autonomous weapon systems, the coordination of drone swarms or *"loyal wingman"* systems already under development (UAVs that accompany piloted fighter jets) and the integration of classic military units with robotic systems logistic support or fire concentration.
Development of modelling and simulation capabilities, including in the *"digital twins"* field	These capabilities allow the detailed analysis of multifactorial security, including in the cyber domain, of complex systems or systems-of-systems, including at the level of cities or at the level of widely distributed critical infrastructures, such as electricity networks.

AI technology can be used for autonomous weapon systems, the coordination of drone swarms or "loyal wingman" systems already under development and the integration of classic military units with robotic systems logistic support or fire concentration.

In addition to the research priorities, the authorities, along with other stakeholders, should act to develop a resilient cyber solution ecosystem that provides supply chain security for critical infrastructure operators. With this in mind, we recommend fostering a dynamic private sector, not just through university-based hubs that encourage new start-ups (supply side), but also through demand side policies that generate more demand for cybersecurity related products

and services in an expanding array of domains, including those undergoing late digitalization such as the construction industry (there is even a paradigm called Construction 4.0, based on the automation of the architecture, engineering, construction and facilities operation sector) (de Soto et al., 2022).

CONCLUSIONS

Omnipresent digitalization is generating a systemic impact on the functioning of critical infrastructures and, consequently, on the production of critical goods and services. On the one hand, it creates new efficiencies and new capabilities, allowing tighter integration of complex infrastructure systems-of-systems across geographic areas, domains, and value chains. On the other hand, it generates new risks, vulnerabilities and threats. Decision-makers, legislators and policymakers are trying to advance the framework for security governance to respond to the new circumstances, but technological change and the implementation happen faster than our capacity to adapt our awareness of the problem and improve our security culture.

We recommend fostering a dynamic private sector, not just through university-based hubs that encourage new start-ups (supply side), but also through demand side policies that generate more demand for cybersecurity related products and services in an expanding array of domains, including those undergoing late digitalization such as the construction industry .

The CIP framework provides a useful way to gauge the overall impact of digitalization. We have underscored the systemic transformations in the cyber field, the evolution of the cybersecurity and environment. Moreover, we have defined transversal approaches including the impact of new legislative developments at EU level and a possible national agenda for cyber development.

Future research will require new capabilities in modelling and simulation, their integration into business and governance processes, as well as adequate strategies and plans for dealing with the introduction of new technologies such as AI, quantum computing and blockchain.

BIBLIOGRAPHY:

1. Bucoveţchi, O., Simion, P.C. (2015). *Importance of interdependencies in critical infrastructures' protection.* UPB Scientific Bulletin, Series C: Electrical Engineering and Computer Science, 77 (1), pp. 301-309.
2. Chen, J., Lu, Y., Zhang, Y., Huang, F., Qin, J. (2023). *A management knowledge graph approach for critical infrastructure protection: Ontology design, information extraction and relation prediction*. International Journal of Critical Infrastructure Protection, 43, art. no. 100634, doi: 10.1016/j.ijcip.2023.100634.
3. *Cybercriminals Today Mirror Legitimate Business Processes*. *Fortinet Cybercrime Report 2013*. Fortinet, https://cybersafetyunit.com/download/pdf/Cybercrime_Report.pdf, retrieved on 12 January 2024.
4. De Soto, B.G., Georgescu, Al., Mantha, B., Turk, Ž., Maciel, A.&Sonkor, M.S. (2022). *Construction cybersecurity and critical infrastructure protection: new horizons for Construction 4.0*. ITcon, vol. 27, pp. 571-594, https://doi.org/10.36680/j.itcon.2022.028, retrieved on 22 January 2024.
5. European Commission (2023). Digital Economy and Society Index 2022, https://digital-strategy.ec.europa.eu/en/policies/desi, retrieved on 12 January 2024.
6. Georgescu, Al., Bucovețchi, O. (2023). *Protecția Infrastructurilor Critice – abordări conceptuale.* Craiova: Editura SITECH, ISBN 978-606-11-8547-4.
7. Gheorghe, A. V., Georgescu, A., Bucovețchi, O., Lazăr, M., & Scarlat, C. (2018). *New dimensions for a challenging security environment: Growing exposure to critical space infrastructure disruption risk*. International Journal of Disaster Risk Science, 9, 555-560.
8. Katina, P.F., Keating, C.B. (2015). *Critical infrastructures: a perspective from systems of systems*. International Journal of Critical Infrastructures, no. 11:4, pp. 316-344.
9. Mehta, B., Reddy, Y. (2015). *SCADA systems.* In *Industrial Process Automation Systems*. Elsevier, pp. 237-300. Doi: 10.1016/B978-0-12-800939-0.00007-3.
10. Nazir, S., Patel, S., Patel, D. (2017). *Assessing and augmenting SCADA cyber security: A survey of techniques*. Computers&Security, 70, pp. 436-454, doi: 10.1016/j.cose.2017.06.010.
11. O'Gorman, B., Wueest, C., O'Brien, D., Cleary, G., Lau, H.&Power, J.P., Corpin, M., Cox, O., Wood, P., Wallace, S. (2019). *Internet Security Threat Report.* Vol 24, Symantec, https://docs.broadcom.com/doc/istr-24-2019-en, retrieved on 22 January 2024.
12. Vevera, A.-V. (2022). *A transversal analysis of the cyber domain in critical infrastructure protection (Abordarea transversală a domeniului cyber în protecția infrastructurilor critice).* București: Editura Militară, ISBN 978-973-32-1275-1.
13. Vevera, A.V., Cîrnu, C.E., Rădulescu, C.Z. (2022). *A Multi-Attribute Approach for Cyber Threat Intelligence Product and Services Selection*. Studies in Informatics and Control, 31 (1), pp. 13-23. Doi: 10.24846/v31i1y202202.

THE IMPACT OF SPACE-BASED CAPABILITIES ON THE GLOBAL BALANCE OF POWER, IN THE CONTEXT OF TECHNOLOGICAL AND MILITARY FIELD RECENT DEVELOPMENT

Colonel (r.) Romică CERNAT, PhD

Research Associate, "Grigore Gafencu" Research Centre for International Relations and Cultural Studies, "Valahia" University, Târgoviște

10.55535/RMT.2024.3.7

After the Second World War the technological progress in space systems has increased the relevance of the space domain, which has an essential strategic role in obtaining victory in all battlespace domains. Space capabilities perform a decisive role in all types of military operations, especially those involving the employment of nuclear weapons, in early warning, identification, location of nuclear facilities and launching sites, as well as in destroying them, in support or intermediary operations, collecting information in all warfighting domains, surveillance, reconnaissance, management and coordination of operating systems.

Space-based capabilities are also relevant to the normal functioning of modern societies and can be used in activities characteristic to the entire political, economic, civil, information, cyber, infrastructure, and military spectrum. Thus, their interruption would lead to the suspension of the services on which a functional system, for example a state, its society, or departments depend.

Keywords: space-based capabilities; satellites; sensors; detection; surveillance; tracking;

INTRODUCTION

The goal of NATO and its partner states is to keep up with and overcome the challenges generated by the complex future warfare, by capitalizing on the emerging technologies capabilities to enhance the ability to conduct multi-domain operations. (Diaz, 2021, pp. 2-4).

Space-based capabilities – the capabilities using space systems, which support, among others, military commanders, staff, and forces in all operational domains – influence daily activities, especially in advanced societies. These capabilities provide functions and activities that exert influence on the places of residence, transport, energy networks, banking systems and global communications. Satellites assure access to a wide range of information and provide an extensive scope of services in real time, from knowing the latest news to monitoring and coordinating the actions of armed forces in any geographical area during the day or night. (Congressional Research Service, 2024, pp. 1-2). The great powers' rivalry for supremacy in the domains of military actions has been highlighted since ancient times: in antiquity for the ground domain; in the medieval period it was supplemented with the maritime domain; the beginning of the 20th century was marked by the competition of the great powers (UK, USA, Japan, Germany, USSR, Italy and France) to dominate the ground, maritime and air domain, which had as a result two world wars; at the Warsaw Summit, in 2016, NATO recognized cyberspace as a domain of operations, cyber defence becoming part of NATO's core tasks of deterrence and defence; during the Cold War, the USA and the USSR found out a new confrontation domain – the space. (International Relations, 2022, pp. 398-408).

Space-based capabilities provide functions and activities that exert influence on the places of residence, transport, energy networks, banking systems and global communications.

Starting with the end of the 20th century and particularly in the 21st century, space has become more and more militarized. The way of waging warfare – through the employment of multidomain operations – will deeply change in the near future. In modern war, military actions will be multidomain, interconnected, and space will have a relevant

role. The first evidence of transforming the way of waging warfare was the Gulf War (1990-1991), also called ***The First Space War***, in which the U.S. Armed Forces victoriously employed space-based capabilities in the following domains: Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) as well as in electronic intelligence (European Parliament, 2014, pp. 13-17). Since then, space has become a domain of military actions. As a result, other great powers such as the Russian Federation and the People's Republic of China have developed space-based capabilities to diminish U.S. space supremacy. At the same time, the USA has developed its counter-space capabilities to preserve its superiority. The space has become important not only for the military field but also for commercial and civil activities. Consequently, the great powers are developing space-based and counter-space capabilities to accomplish their national interests. (International Relations, 2022, pp. 397- 408).

The first evidence of transforming the way of waging warfare was the Gulf War (1990-1991), also called The First Space War, in which the U.S. Armed Forces victoriously employed space-based capabilities in the following domains: Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) as well as in electronic intelligence.

Today, strategic competitors confront in all domains – physical, concrete domains: land, sea, air, space, as well as abstract domains: cyberspace, electromagnetic spectrum, information environment and the cognitive dimension. Therefore, the military and economy must be performing to deter and, if necessary, defeat potential opponents (Strategic Studies Institute, 2023, pp. 17-18). The space is used not only for military purposes but also for communications, weather forecasts, financial transactions and navigation, being also a potential source of natural resources, an important aspect for all states. (International Relations, ib.). In 2022, about 50 states and multinational organizations possessed and controlled the functioning of over **5,400** artificial satellites that orbit around the Earth. (Statista, 2022, p. 1).

Strategic adversaries such as the USA, Russia, and China and their allies integrate the use of emerging technologies in military operations according to their strategy and doctrine. They are developing capabilities to support the denying of the current global order through multiple layers of parity in all domains – land, air, naval, space, and cyber, a situation that involves defeating the opponent in all the specific layers of each domain to provide coherence of the actions and to obtain victory. (The U.S. Army, 2018, pp. i-viii, 5-15). They use the space domain to obtain operational, logistical and information advantages. In addition to the extension of conventional forces, they quickly improve and harmonize their space, counter-space, cyber, electronic, and information warfare capabilities. (U.S. Department of Defense, 2022, pp. 1-2, 63). The strategic competition, including in the space domain, is an assiduously long-term battle that takes place between two or more opponents that follow incompatible interests, which does not mandatorily imply triggering an armed conflict against the other competitors. Standard and friendly competition between allies, strategic partners, and other international actors that are not potentially hostile does not belong to the domain of this concept. (The Joint Chiefs of Staff, 2023, pp. i-ix).

The article will analyse the purpose of space-based capabilities in the implementation of the great powers' security and defence policies in the global balance of power. At the same time, it will be assessed the way of using these capabilities by the main international actors to promote specific interests. It can be seen a powerful connection between the following domains: ***space***, ***sovereignty***, and ***security issues***. This connection is more obvious than ever given that the greatest amount of data and information at present employed in military and security fields have as a source or utilize space-based capabilities. (European Parliament, 2014, pp. 12 -17).

Space-based capabilities have demonstrated not only during military operations but also in daily activities that they are much more efficient than land, naval, or air-based platforms and thus have a relevant contribution to the consolidation of both internal and external security. Space-based capabilities, among other things, include Earth observation satellite constellations, satellite navigation systems, intelligence satellites, and early warning space-based systems. All these systems, starting with the launch on orbit, are considered critical infrastructures, which entails complete protection, against both intended attacks and other actions. Protecting these platforms requires the development of a *Space Situational Awareness* capability, with the mission to monitor and counter the probable threats for both space-based capabilities and ground-related infrastructure.

Space-based capabilities include Earth observation satellite constellations, satellite navigation systems, intelligence satellites, and early warning space-based systems. All these systems, starting with the launch on orbit, are considered critical infrastructures, which entails complete protection, against both intended attacks and other actions.

Space capabilities represent the possession of the assets and expertise to access, employ, and participate in the space' specific

infrastructure, as well as the capacity to exploit and use the common space-based natural resources. The resources involve the electromagnetic spectrum and the especially necessary space that is occupied by the satellites' orbits (slot allocation). The infrastructure associated with space encompasses satellites and ground-based systems. Common natural resources – in the future – will probably comprise diverse raw materials from asteroids or the Moon, such as metals and water, which would contribute to the Earth-based industry or amplify *"in space"* activities such as manufacturing in space, tourism, operating bases on the Moon and Mars, and so on. (Center for Global Development, 2023, pp. 11-17). Some companies intend to harvest asteroids in space for water and metals, such as the platinum group metals.

The great powers adapt their policies on defending national security regarding the space domain according to national interests. In the last period, military strategists have perceived the space as an operational domain – an area in which offensive and defensive military operations can be conducted – similar to the other domains: land, air, maritime and cyberspace.

The military operations conducted by modern armed forces depend on and exploit the superiority provided by the spatial capabilities and the outcomes of their actions to strengthen the effectiveness of the forces' actions in all domains. Space capabilities ensure a real-time awareness of the situation of own and adversary forces; provide the employment of communications at the global scale; ensure precise and accurate targets employment; support the conduct of expeditionary operations, the deployment in the theatre of operations, movement and manoeuvre; and provide communication flows for cyber electromagnetic operations that support the conduct of joint military actions. These capabilities have a decisive role in the success of large-scale combat actions by ensuring command and control, reliable communications, protected by or not exposed to dangers or risks in extended areas that do not have specific modern infrastructure. (U.S. Department of the Army, 2019, pp. v, 1-1-1-11).

The great powers adapt their policies on defending national security regarding the space domain according to national interests. In the last period, military strategists have perceived the space as an operational domain – an area in which offensive and defensive military operations can be conducted – similar to the other domains: land, air, maritime and cyberspace. (Congressional Research Service, 2024, pp. 1-3).

SATELLITES – CHALLENGES AND PERSPECTIVES

This chapter explains the importance of satellites in today's world. Space has become of decisive importance, having significance not only for the state's national security but also for the daily life of modern society, while also representing a generating threats domain where an increasing number of states and private entities are active.

The space domain is defined as the area above the altitude where the atmospheric effects on airborne objects become negligible. The space domain is a physical area in which military, civil and commercial spatial activities are carried out, and the upper limit extends infinitely outward. The armed forces joint and space operations are impossible to be divided or separated. The typical brigade battle array has over **2,500** positioning, navigation, and synchronization devices and over **250** satellite communication devices employed to execute precise striking, movement, manoeuvre, communications, protection, command and control, and other battle requirements. *The Karman line is a proposed conventional boundary between Earth's atmosphere and outer space set by the International Aeronautical Federation at an altitude of **100** kilometers above mean sea level*. A satellite is an object, which crosses the Karman line, on which a single force acts – gravity, and which moves at a speed of at least **8** km per second, to keep in orbit. (U.S. Department of the Army, 2019, pp. v, 1-1-1-11). ***Artificial satellites are human-made objects deliberately placed into orbit***.

The space domain is a physical area in which military, civil and commercial spatial activities are carried out, and the upper limit extends infinitely outward. The armed forces joint and space operations are impossible to be divided or separated.

In creating and maintaining superiority in space, a special role is played by the specific capabilities of electronic warfare, missile launch warning, intelligence, surveillance and reconnaissance, command and control, and cyber and space domain awareness – knowledge or perception. Data collection and advanced analysis tools provide real-time information and advantages in the timely decision-making process. The offensive and defensive cyber capabilities provide protection to space missions and deter adversaries, while satellite technologies, planned or conceived to accurately notify ground troops about the interruption or undermining of the global positioning system (GPS), provide data that ensure a perspective on the situation and advanced awareness in anti-access or denied areas. (O'Brien, 2023,

p. 1). Generally, the national security space capabilities, those that provide communications as well as those used for intercontinental ballistic missile attack warning, probably remain positional/stationary. They, unlike those stationed into the orbit, probably spend most of their lifetime transforming their energy situation and performing manoeuvre operations. This system is made up of satellites that have an orbit located near those with geosynchronous orbit, being intended for space surveillance operations, monitoring the functioning mechanism of other platforms, observing the deviations from a normal, correct functioning, the possible dysfunctions, or the possibly suspicious or aggressive course of action of certain satellites belonging to the opponents. This dynamic, more manoeuvrable approach favours the surprise by gaining the initiative against opponents. The Ukraine conflict has pointed out, in particular, the relevance of space capabilities for surveillance and communications. Russia has tried to jam the GPS and navigational satellite systems used by Ukraine, and Ukraine responded by similar measures (Vergun, 2023, pp. 1-2).

The Ukraine conflict has pointed out, in particular, the relevance of space capabilities for surveillance and communications. Russia has tried to jam the GPS and navigational satellite systems used by Ukraine, and Ukraine responded by similar measures.

Tracking and detecting traditional ballistic missiles and manoeuvring hypersonic weapons, which can fly at speeds over **Mach 5,** involve developing a much more powerful network of satellites that will be located in the low Earth orbit, about **2,500** km above the surface of the planet. For better efficiency, the tracking satellites will be launched into the same orbit with tracking hypersonic and ballistic missile space sensors. Thus, they can survey the targets in the same orbit, favouring the common operating of the two types of sensors. (Albon, 2024, pp. 1-4). Maintaining an advantage in future wars is favoured by the space-deployed capabilities – reconnaissance and spy satellites, communications relays, and navigation-supporting assets – utilized by field, sea, and air combatants. (Demarest, 2023, pp. 1-2).

With the introduction of two-way radio stations, military actions, weapons systems, and data transmission/reception applications have become **electromagnetic spectrum**-dependent. Applications comprise: *radio frequencies to communicate with own forces; microwave for transmission of tactical data, radars, and satellite communications; infrared for information collection and the targets*

acquiring; and lasers throughout the full spectrum to communicate, transmit data, and possibly destroy a target. The equipment ensures communication and data transmission, providing timely information necessary for navigation, command and control of forces anywhere on the globe. Current military operations also depend on electronic combat capabilities deployed on satellites, for early warning and surveillance in an extended zone, communications, command and control. Platforms with this destination comprise constellations of infrared systems arranged in space, electronic satellites for collecting information, and radar systems arranged in space. (Congressional Research Service, 2022, pp. 1-2). The employment of data provided by satellites and satellite communications contributes to the development of a resilient society, supporting disaster and crisis management as well as assessing the consequences of climate change.

Current military operations also depend on electronic combat capabilities deployed on satellites, for early warning and surveillance in an extended zone, communications, command and control. Platforms with this destination comprise constellations of infrared systems arranged in space, electronic satellites for collecting information, and radar systems arranged in space.

The new race on the space domination is in progress. Hundreds of satellites are launched into the Earth's orbit every year for different purposes: ***communications*** and ***the Internet of "things"*** (data collection and exchange), ***navigation/GPS***, ***commercial***, ***government administration***, ***military***, ***environmental monitoring***, ***technological development***, ***civil***, with ***combined purposes*** and ***border security***. Thousands of non-functional satellites orbit around the planet as a spatial waste. In total, there are nearly **8,000** satellites surrounding the planet and this number continues to grow (Science Alert, 2023). In the present era, governments have realized that there are huge advantages and numerous applications that use space capabilities. Thus, satellites represent critical infrastructure for many government activities as well as for daily activity in a society.

Indeed, many organizations, associations, institutes, and bodies monitor, study, and estimate the situation of satellites. They have figures, reference systems and classifications that vary for the same analysis data. For the most realistic information, given that there is no *Treaty regarding space capabilities*, the article presents data on satellites from several sources. Four years ago, there were almost **6,000** satellites orbiting around the Planet and about **60%** of them were no longer working becoming space waste. The Union

of Concerned Scientists (UCS) established that **2,666** operational satellites surrounded the globe in April **2020** (Euroconsult, 2021). In the coming years, Euroconsult has assessed that about **990** satellites will be launched every year. It entails that there could be **15,000** satellites in orbit by 2080 (Ib.).

Most operational satellites belong to the commercial field. About **61%** of them are assigned for communications, including a wide range of connectivity satellites from satellite television and the Internet of Things, to the global internet: streaming (a method of transmitting or receiving data, especially video and audio, on a network of computers as a constant flow); video calls; online gaming; remote working and many more are now possible even in the most remote locations, due to the most advanced internet system in the world. After communications, **27%** of commercial satellites were launched for Earth observation reasons, including environmental monitoring and border security. Commercial satellites can perform different missions, thus, for some time, a satellite may have a task to monitor a contested border and, later, can monitor possible mining works, and then the consequences of a natural disaster. (Wood, 2020, pp. 1-5).

Most operational satellites belong to the commercial field. About 61% of them are assigned for communications, including a wide range of connectivity satellites from satellite television and the Internet of Things, to the global internet: streaming; video calls; online gaming; remote working and many more are now possible even in the most remote locations, due to the most advanced internet system in the world.

The USA, ranking first in April **2020**, operates almost half of all the satellites, namely **1,308**, China follows in the second position with about **356** satellites, and Russia is the third with **167** satellites in operation, followed by the United Kingdom with **130** satellites ranking fourth. The USA and the USSR (now the Russian Federation) led the space race between the 1950s and 1960s, finding at this time among the first three satellite operators. The data provided by experts of the UCS show that at the time of analysis – **5 May 2023** – there were over **7,560** operational satellites in the Earth's orbit. Of them **5,184** belonged to the USA (Commercial: **4,741**, Military: **246**, Government: **167** and Civil: **30**), **181** to the Russian Federation, **628** to China, and **1,572** to other states. The United States of America, China, and Russia are the states that have dominated the Earth's orbit ranking first on the list of operational satellites. Details are presented in *table 1*.

Table 1: The situation with all Earth's artificial satellites.
(Wood, 2020, pp. 1-5, Union of Concerned Scientists, 2023, pp. 1-3, Pixalytics, 2023, pp. 1-15).

Operational satellite by type \ Year		2020 – v.c.	% operational	Jan. 2023 pix./ucs	May 2023 ucs
Commercial	Communications	1,007	61%	4,823	
	Earth observation	446	27%	1,167	
	Navigation/GPS	97		155	
	Tech demonstration & development	87		414	
	Space science / observation			109	
	Earth science			25	
	Other	9		25	
	All commercial satellites (including combination)	1,646/ 1,440	54%	5,280	
Government		436	16%	688	
Military		339	13%	588	
Civil		133	5%	162	
Combination (Other)		112	4%		
Combination (Commercial)		206	8%		
USA		1,308		4,511	5,184
China		356		586	628
Russia		167		177	181
UK		138		561	
Other		697		276	1,572
TOTAL		2,666	100%	6,718	7,560
The Low Earth-orbit		1,918			6,768
The semi-synchronous orbit		137			143
Elliptical		57			59
Geosynchronous orbit		554			590
Defunct satellites		3,200			

Government and civil goals represent **21%** of the total operational satellites of the Earth, and the military purposes are **13%**. ***SpaceX***, founded by Elon Musk, is not only a launch provider for missions to the International Space Station but also the largest commercial operator of satellites on the planet. In July 2020, Amazon was granted approval by the Flight Procedure Program to launch and operate an internet constellation (a group of satellites) of **3,266** satellites (EU Court of Justice, The Year Review, 2020).

Details about the origin country of the satellites that orbit around the Earth are presented in *figure 1*.

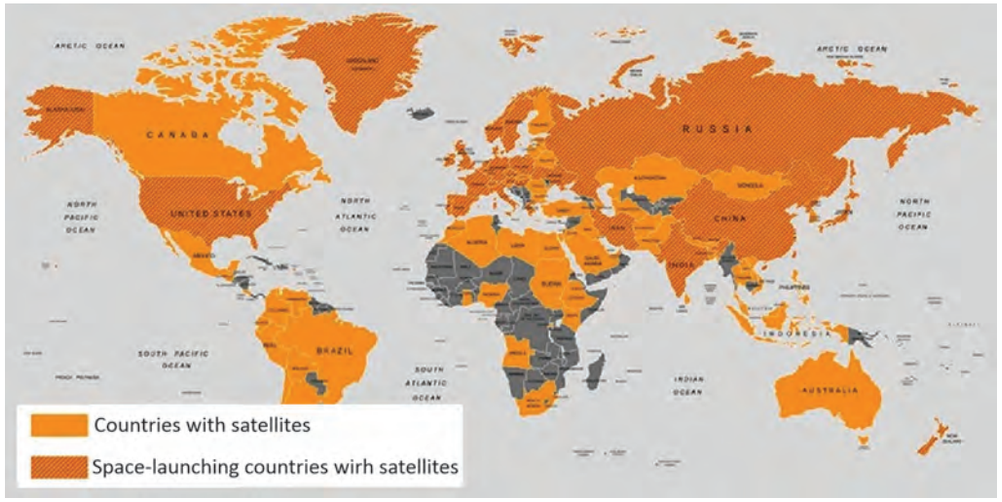


Figure 1: The situation with the states owning satellites
(Union of Concerned Scientists, 2023, pp. 1-3).

According to *The Index of Objects Launched into Outer Space*, updated by the United Nations Office for Outer Space Affairs, at the beginning of July **2023**, around the Earth orbited **11,330** individual satellites. A **37.94%** increase compared to January **2022**. (Pixalytics, 2023, pp. 1-15). The following types of devices are sent to space: satellites, crewed spacecraft, probes, and space station flight equipment.

The satellites and the Earth's ecosystem provide continuous, rigorous scientific data, which evaluates the Earth's surface change. With the help of advanced algorithms that process the data provided by the remote-controlled constellation of satellites, valuable information about water, temperature, carbon and vegetation are obtained.

The capabilities that provide data from the entire electromagnetic spectrum, including optical sensors, radars, passive microwaves, and LIDAR sensors (measures the distance to the nearest obstacle and uses light from a laser), provide different aspects of the physical properties of the Earth. About 200 *Dove* satellites permanently offer a high-resolution [3.7-meter resolution images in four multispectral bands: RGB (red, green, blue) and Near Infrared], continuous and complete image of the Earth's surface. They provide greater visibility, more timely, continuous coverage, evolution by design, and access and integration. Over 300 million square kilometres of imagery are collected each day. (Visual Capitalist, 2024, pp. 1-5).

The orbit of the Earth is separated into three distinct areas. The Low Earth-orbit, the area between **200-2,000** km above the Earth. The semi-synchronous orbit is the area between **10,000** to **20,000** km above the Earth's surface. This orbit is generally used by navigation and communications satellites. Geosynchronous orbit is the area located over **36,000** km above the Earth's Equator surface. The telecommunications and weather satellites in this area can remain in orbit for millions of years. Therefore, the lower the orbit is, the less time is likely to stay in space. (Bhutada, 2021, pp. 1-6).

The orbit of the Earth is separated into three distinct areas. The Low Earth-orbit, the area between 200-2,000 km above the Earth. The semi-synchronous orbit is the area between 10,000 to 20,000 km above the Earth's surface. This orbit is generally used by navigation and communications satellites. Geosynchronous orbit is the area located over 36,000 km above the Earth's Equator surface.

THE ROLE OF SPACE-BASED CAPABILITIES IN THE SUCCESS OF MILITARY OPERATIONS, DETERRENCE AND DEFENCE OF NATIONAL SECURITY

This chapter exposes the potential employment of space-based capabilities to promote each state's interests. In the military field, space is critical for the competition and the military actions leading in each domain. Space capabilities ensure the notification about the ballistic missiles' employment and their tracking, critical aspects for the national security of each state, and provide data on the target's location and the optimal moment to strike it accurately. It also ensure the continuity of communications in an environment with extreme conditions to carry out the command and control at the military action's theatre and global level, decisive elements for modern war. Great powers are developing progressively sophisticated capabilities for denying and neutralizing the assets that support the opponents' space missions. As a result, the means of counteracting the space capabilities have diversified, modernized and adapted

to the requirements of the present. China has, by this time, deployed ground-based platforms that have the mission and capacity to act against space capabilities. Moreover, it develops programmes for creating or designing new assets and methods in order to disrupt and neutralize the U.S. space capabilities, to achieve a complex structure of space capabilities for supporting armed forces in the execution of strikes at long distances, and precisely to limit the U.S. capacity to carry out joint operations in the Indo-Pacific area. Russia also develops, tests, and deploys the kinetic space-based capabilities as well as ground-based with the mission to neutralize the U.S. space capabilities. The space at this time is an increasingly challenged area by great powers that have space-based capabilities able to trigger activated attacks from space on air, terrestrial and naval forces. (Vergun, 2023, pp. 1-2).

Space operations are those operations that have a strong effect on or employ space-based and ground-based capabilities to strengthen the power to take military actions and deterrence.

Space operations are those operations that have a strong effect on or employ space-based and ground-based capabilities to strengthen the power to take military actions and deterrence. (U.S. Department of the Army, 2020, pp. i-xii). Lately, there is information according to which Russia is developing a nuclear weapon to be carried out in space, planned or conceived to disable or destroy the adversaries' satellites. Sufficient data on the missions and characteristics of such a weapon are not public, namely it is not known if it involves the detonation of a nuclear explosive in space or is another anti-satellite capability, powered by a nuclear reactor in space. (Tingley, 2024, pp. 1-2).

The systems for neutralizing space capabilities include kinetic physical means (direct ascent weapons – missiles – scheduled to intercept a satellite and co-orbital that initially is launched on orbit, for example, satellites, and after being activated execute the necessary maneuvers for striking the target), non-kinetic physical (lasers, high-powered microwave weapons, and nuclear weapons detonated in space that create an electromagnetic impulse), electronic (jamming or spoofing radio frequency signals by which space capabilities transmit and receive data) and cyber-targets (the data itself). (Congressional Research Service, 2021, pp. 1-3). In this context, the ability of a state to attribute, unequivocally, a missile attack to an adversary and to select the appropriate and efficient response means becomes critical. Equally important are the capabilities in space or ground that can achieve the deterrence and defence of national security.

The threat represented by the use of ballistic missiles is increasingly present, including by adversaries that do not have great power status, such as North Korea and Iran. These states have proven that they own technologies, such as controlled and guided re-entry vehicles, and in the short term could diversify re-entry vehicles, decoy missiles and other countermeasures to mislead the interception and strike assets after the boost phase. The progress in ballistic missile threat has led to an increase in the importance of satellites, sensors, platforms and capabilities for missile intercepting and detonating starting with the boost phase. The development of detection capabilities, like lightweight gallium nitride-based radar, can result in increasing the radar air platform's role and efficacy, reducing, accordingly, the gaps in detecting and tracking, triggering the neutralization planning situation of the ballistic missiles in the boost phase. Progress in resolution and image processing by infrared sensors can additionally compress the detection timelines of satellites, in the future. Timing, continuous missile tracking, immediately after launch, is a priority for any missile defence system in the boost phase. A constellation of sensors in the boost phase should comprise a complex of platforms and types of sensors to provide prompt detection and tracking. The prompt selection of the timing and place of the missile' striking is also critical for its neutralization in the boost phase and involves a layered defence to preclude the inefficient employment of midcourse trajectory interceptors or to support successful target engagement, many times, in the boost phase. A space-based interception system is the exclusive variant to place interceptors in a sufficiently close layer for the boost phase to neutralize intercontinental missiles. The progress achieved through miniaturized sensors, avionics, and turbo pumps results in the decreased weight of the part designated for target detonation and implicitly the total interceptor mass. To be efficient, space-based interceptors must be provided with protection measures against the adversaries' anti-satellite modern methods and means. (Karako, 2022, pp. 6-7, 15-36, 43).

The threat represented by the use of ballistic missiles is increasingly present, including by adversaries that do not have great power status, such as North Korea and Iran. These states have proven that they own technologies, such as controlled and guided re-entry vehicles, and in the short term could diversify re-entry vehicles, decoy missiles and other countermeasures to mislead the interception and strike assets after the boost phase.

Land, sea, and space-based sensors, including satellites and radars, provide *The Ballistic Missile Defence System* with the ability to detect, track, and discriminate incoming ballistic missiles. Details are presented in *figure 2*.

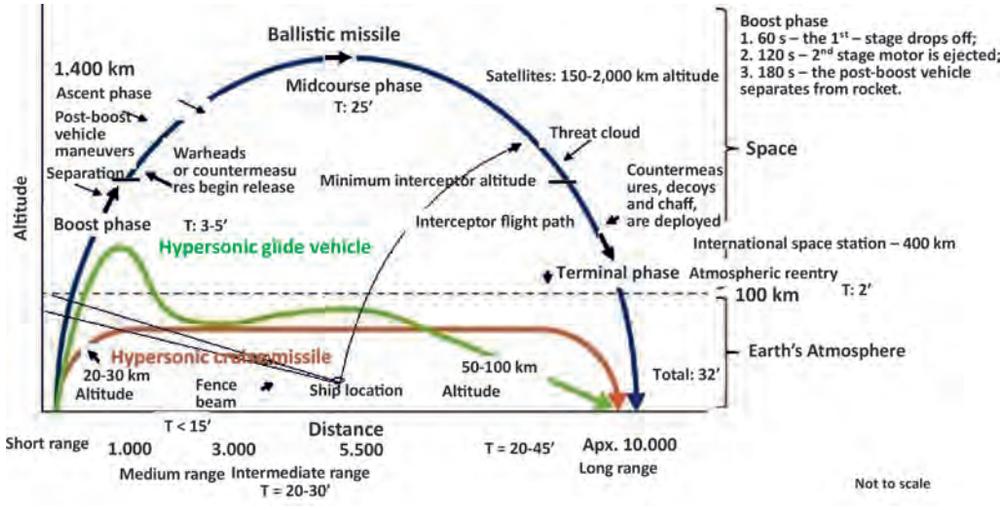


Figure 2: Missile trajectories, their actions during the flight and the reaction of the air and missile defence system
(Kunertova, 2021, p. 55; Bhutada, 2021, pp. 1-6; Karako, 2022, p. 1-7, Boord, 2016, pp. 36, 63, 99).

It was during the Cold War when the U.S. and Soviet governments were in a race to show their technological superiority in the new arena of outer space. The race continued even after the end of the Cold War, the main milestones of this race being as follows: in 1961 The Soviet Union put the first person (Yuri Gagarin) in space; in 1969 first crew landed on the Moon (Apollo 11); in 1981 a reusable spaceship: NASA space shuttle era began; in 2000 the International Space Station welcomed its first crew. It is the most expensive structure ever built; 2004 the new age of commercial space lift started. Spaceship One sent a manned flight to suborbital space and back twice in the span of five days; in 2010 Space Exploration Technologies (Space X) led by Elon Musk launched its Dragon Capsule atop a Falcon 9 rocket; Space X was the first private company to launch a spacecraft to orbit and recover it after re-entry; in 2011 NASA retired the space shuttle after 30 years of operations.

Here are some key players in today's space industry that are vying for private sector space supremacy: ***Old Guard*** consisting of juggernauts such Boeing, Lockheed Martin, and orbital scientists; ***Orbital:*** founded in 1982 is one of the most established companies in the space sector that has operated over 1000 satellites, launch vehicles, and other space-related systems since inception; ***Lockheed Martin*** is a juggernaut

in the aerospace and defence industries and space capable builder; ***Boeing*** is another deep-pocketed aerospace company with ties to space; ***United Launch Alliance (ULA)*** is a partnership between Lockheed Martin and Boeing formed in 2006; ***SNC/Sierra Nevada Corporation*** is developing the *Dream Chaser*, a re-usable space plane designed to carry up to seven people to and from low Earth orbit. Launching vertically on ULA's Atlas V rocket it would land horizontally on a conventional runway; ***Scaled Composites*** was founded in 1982 to develop experimental aircraft; ***New Guard*** is typically founded by billionaire entrepreneurs and aims to reduce costs and develop new technologies; ***Space X***, founded in 2002 by former Paypal entrepreneur and Tesla Motor CEO, Elon Musk, is unquestionably the industry leader, currently operating the largest fleet of satellites in orbit – about 50% of the global total. (Desjardins, 2014, pp. 1-12).

Anti-satellite weapons are weapons that are designed to deceive, disrupt, deny, degrade, or destroy space systems. Around the Earth are orbiting thousands of satellites that contribute to the normal management of activities in the following fields: commercial, civil, strategic and military. The national security and the global balance of power are decisively influenced by the proper functioning of these space capabilities, so some states have developed anti-satellite weapons that can be used to suppress or destroy satellites in orbit. For these military actions, non-destructive means are used, such as cyber attacks or lasers to interrupt the functioning of satellites or destructive means that produce high-speed physical clashes to break the satellites into thousands of fragments that seriously affect the optimal functioning of other spatial capabilities and that can orbit the Earth for decades at extremely high speeds. According to the UCS, the destruction of a single **10**-ton satellite can generate: **8** to **14** million debris pieces between **1** mm and **1** cm in size; **250,000** to **750,000** debris pieces between **1** cm and **10** cm; **5,000** to **15,000** debris pieces greater than **10** cm. Already in space there are about **8,800** metric tons of flying spatial debris. This spatial waste can travel at speeds up to **29,000** km/h (about 8 km/s). At this speed even fragments of millimetre sizes are serious threats for other objects in orbit. The outer space of the Earth is populated with millions of pieces of artificial debris, sometimes arranged in large and dense groups, which represents potential dangers for other functional capabilities. With the launch of the Soviet satellite Sputnik in **1957** the race for supremacy in space was triggered. It also

Anti-satellite weapons are weapons that are designed to deceive, disrupt, deny, degrade, or destroy space systems. Around the Earth are orbiting thousands of satellites that contribute to the normal management of activities in the following fields: commercial, civil, strategic and military.

led to the accumulation in space of large or small pieces of inert metal. Inactive satellites, the upper stages of the launch vehicles, the disposal of fragments resulting from uncoupling, and even frozen clouds of water and minuscule paint elements continue to exist in orbit beyond the Earth's atmosphere. If one fragment impacts with another, more scraps are discharged. It is estimated that approximately **21,000** fragments of space waste greater than **10** centimetres and half a million fragments of waste between **1** cm and **10** cm are assessed to move around the planet and their number will increase. In space, there are in addition millions of waste fragments smaller than one-third of one centimetre. In the Low Orbit of the Earth, the objects are moving at a speed of **7** km per second. At this speed, a small fragment of paint stores the same energy as a **300**-kilogram object that moves at a speed of **100** km per hour. The impact of critical space technologies with such an object can damage essential components, such as pressurized devices, solar cells, or internet connection devices, but can also generate new scraps that can cause damage. In the last 50 years, space pieces of debris have resulted from the accidental explosion of objects.

The armed forces of the USA, Russia and China have the needed capabilities to monitor space debris even if they are small in size. Objects up to about 10 cm can be detected by Earth's radars or optical telescopes.

The armed forces of the USA, Russia and China have the needed capabilities to monitor space debris even if they are small in size. Objects up to about **10** cm can be detected by Earth's radars or optical telescopes. Before each launch, the potential orbit of the satellite is screened to avoid possible collisions with fragments of spatial waste. Moreover, the crews of the space shuttles and the International Space Station can modify their orbits if the route of a larger object overlaps with that of the station. Anyway, the satellites and spacecraft have provided a protective coating to avoid interrupting vital components' functioning. (Tillman, 2013, pp. 1-5).

There are only four states – Russia (former USSR), China, USA, and India – that have successfully, **15** times, experienced the two categories of destructive anti-satellite weapons. ***Type one***: co-orbital, weapons that are placed in orbit, perform manoeuvres until they reach a favourable position towards the target and use different means – direct collision, fragmentation, or use of robotic weapons – to neutralize it. ***Type two***: direct ascent, missiles that are detonating satellites in orbit are launched from the surface of the Earth or on-air platforms. (Buthada 2022, pp. 1-3). At this moment, a significant increase in threats against space capabilities can be seen. They include the detonation of a nuclear weapon in space, threats of kinetic energy, cyber threats, electronic warfare, space capabilities awareness, denial and deception, directed energy weapons, orbital threats, and ground site attacks. (U.S. Department of Defense, 2020, pp. 3-10). The state defence space architecture implies the existence of the necessary space capabilities to support the actions of the ground, aerial, and naval forces, as well as the missile launch warning, tracking, and neutralization. Diversifying and amplifying the constellations of satellites, the orbits, and the achievement of technological advantages contribute to consolidating the architectural structure.

Given the short flight time of an intercontinental missile to the target, striking it in the boost phase – about five minutes – represents a critical challenge regarding the command and control, the battle management system, signal processing, tighter sensors-shooting integration, the missile defence system, the capabilities of the technical assets – sensors, radars, interceptors, computational technique, directed energy systems, remote-piloted aircraft, striking assets – for detecting, tracking, processing and intercepting a missile. The missile's interval of employment is perceived as a relationship or expression that involves two variables: the time of combustion of the missile propulsion fuel and the compressed time for the missile defence in the calculation of the efficient means of employment, moment and point of the impact. By evaluating all the parameters relevant to the engagement window, in the last 20 years, the following possible engagement openings last from **175** to **235** seconds for slower-accelerating liquid fuel and **125** to **151** seconds for faster, solid fuel. Delays determined by detection and tracking lead to additional requirements for other systems, such as the interceptor speed and range. Theoretically, the interceptor has an average speed of **4** kilometres per second and is launched at an altitude of **15,000** meters. Space-based infrared sensors have the ability to detect a missile after launch at about **45** seconds and after reaching an altitude of **7** km. Once the missile has been detected, a sensor platform must track the missile's flight trajectory to the target and ensure tracking data to the fire control system to determine an interception and detonation point. The space solution with a large coverage, based on a constellation of sensors, interceptors and effectors, arranged in the geographical zone where they can act without limitations, ensures the successful neutralization of missiles. The space-based kinetic

The missile's interval of employment is perceived as a relationship or expression that involves two variables: the time of combustion of the missile propulsion fuel and the compressed time for the missile defence in the calculation of the efficient means of employment, moment and point of the impact.

interceptors do not have the specific constraints of the other domains, but, due to the permanent motion, they cannot stand or track for a long time an area, involving a constellation of such means to achieve a permanent coverage of areas of interest.

The size of the constellation is determined by the area of interest, the duration of the missile trajectory, and the interceptor's speed and effectiveness. A global coverage starts from **3,000** interceptors, and for missiles launched from Iran and North Korea, orbits between **25 - 45** degrees latitude, about two interceptors would be needed in the action range at any time. To neutralize the liquid fuel missiles launched by the two states, a necessary between **240** and **700** interceptors, with interception speeds of **5** - **6** km/s, has been estimated. The operational requirements of the sensors and interceptors are determined by the correlation between the duration and length of the missile trajectory in this phase and the assumptions regarding the location, relationships, interconnectivity and synchronization of the employment assets.

China – one of the most active and capable adversaries in space – doubled the number of satellites. In 2023 they had over 700 operational satellites.

The main landmarks of the engagement process, in which a decisive role is played by the space capabilities, specific to the boost phase are the following: detection (the time required for sensors to register a boosting missile), missile track establishment, engagement planning (the time required for command control and battle management systems to produce an engagement solution), decision time (the time available for human authorities to decide whether or not to engage a target), engagement (the time required for an effector to neutralize an enemy missile), and kill assessment.(Karako, 2022, pp. 1-7, 15-34).

Today's space is a challenging domain. The threats to space capabilities include jammers, anti-satellite weapons, on-orbit grapplers, tracking satellites, *"nesting dolls"* (anti-satellite weapons, stored in each other), directed energy weapons (and) cyber attacks. China – one of the most active and capable adversaries in space – doubled the number of satellites. In 2023 they had over **700** operational satellites. (Pope, 2023, pp. 1-3).

CONCLUSIONS

The space as a domain for carrying out the warfighting actions is relatively new and has special characteristics compared to the other domains. Analogies cannot be made between the strategies, tactics and capabilities specific to the other domains and those specific to the space. The competition in the space domain was triggered with the launch of the first object in space – the transformation of space from the object of study to the domain of carrying out warfighting actions – among the USA, Russia and China. Subsequently, other great powers, state and non-state actors have actively participated in this new competition. In space, as in any domain, offensive and defensive military actions can be conducted similar to land, naval and air. It is increasingly obvious that space – as a domain to deploy space capabilities as well as to conduct or coordinate military actions – decisively influences the sovereign control over the state's security and defence policies and activities, determining a high level of complexity of space security governance as well as of security and defence policies. The viability has already been proved for the dual use of space capabilities for both the military and the normal functioning of society.

Starting with the Gulf War, the latest conflicts have confirmed the determining role of space capabilities in achieving success and the importance of space as a domain of operations. It depends on the great powers if the space can be unpredictable, characterized by chaos and destruction, or, on the contrary, by stability, peace and potentiality. The highest risk is determined by their inability to adapt to the pace required by changing this new domain of military actions. Many of the hypotheses that have determined previous assessments are no longer reasonable. A mixture of new threats, strategic risks, and priorities justify the interest in space and space capabilities. The use of anti-satellite weapons can hinder the usability of orbit, pose a direct threat to other satellites, increase the cost of using space, and escalate political conflicts.

The use of anti-satellite weapons can hinder the usability of orbit, pose a direct threat to other satellites, increase the cost of using space, and escalate political conflicts.

The relatively short ballistic missiles' period of flight together with the very short interval of time in which they must be detected and associated with certain delays in tracking, surveillance, and engagement require a space deployment and higher technical-tactical characteristics for space capabilities as well as effective integration with the ground and space assets for striking. The decrease in missile detection, identification and discrimination time by satellites and sensors as soon as possible after launch and the calculation of the missile hitting point on the trajectory represent critical operational requirements for space capabilities. Sensors with leaps in infrared resolution and image processing have a relevant contribution in reducing detection

time. Also, the modern technologies of semiconductors as well as the perfecting storing and manipulating data processes favoured the smaller, lighter and more reliable radar production and the increase in the number of airborne sensors. All the above aspects, together with the selection of reaction, rules of engagement, system of weapons and hitting point, contribute to the missiles' destruction.

Space capabilities can counteract more complex threats than terrestrial ones and the technical developments make this approach more viable. The progress of space capabilities regarding satellites, sensors, interceptors, lasers, remotely piloted aircraft, image processing, radars, detection and tracking increase their potential to influence the balance of global power. Space capabilities provide the implementation of the operational planning process at a global level as well as the means of approach or entry into limited access or denied areas. Also, favourable conditions are provided for applying the principles and laws of the armed conflicts as well as for the requirements regarding the operation's success, namely, freedom of action, air missions, responsiveness, global approach, flexibility in the use of means, speed, synchronization, unity of fighting actions, manoeuvre, depth and persistence. Space capabilities have a great contribution to achieving relevant activities to obtain battle success: communications, intelligence, missile-warning, surveillance operations, operations against space capabilities using jamming, lasers, destructive kinetic and cyber-attack capabilities and anti-satellite systems. Solar geomagnetic storms can cause operating interruption or even destruction of space-based capabilities with catastrophic effects for humanity in the short, medium, and long term.

Space capabilities have a great contribution to achieving relevant activities to obtain battle success: communications, intelligence, missile-warning, surveillance operations, operations against space capabilities using jamming, lasers, destructive kinetic and cyber-attack capabilities and anti-satellite systems.

BIBLIOGRAPHY:

1. Albon, C. (5 February 2024). *Pentagon launches six satellites to boost missile tracking capability,* pp. 1-4, https://www.defensenews.com/battlefield-tech/space/2024/02/14/pentagon-launches-six-satellites-to-boost-missile-tracking-capability/, retrieved on 27 March 2024.
2. Bhutada, G. (6 October 2021). *Space Sustainability: Preserving the Usability of Outer Space*, pp. 1-6, https://www.visualcapitalist.com/sp/space-sustainability-preserving-the-usability-of-outer-space/, retrieved on 27 March 2024.
3. Boord, W.J., Hoffman, J.B. (17 February 2016). *Air and Missile Defense Systems Engineering*, CRC Press Taylor&Francisc Group, pp. 1-2, 23, 29, 34-39, 41- 43, 49-50, 63, 99, https://www.taylorfrancis.com/books/mono/10.1201/b19671/air-missile-defense-systems-engineering-warren-boord-john-hoffman, retrieved on 15 March 2024.
4. O' Brien, W.A. (19 December 2023). *Space Force leader stake ambitious look at future*, p. 1, https://books.google.ro/books?id=LU3OCwAAQBAJ&printsec=frontcover&redir_esc=y#v=onepage&q&f=false, retrieved on 27 March 2024.
5. Buthada, G., Smith, M. (14 June 2022). *Anti-Satellite Weapons: Threatening the Future of Space Activities*, pp. 1-3, https://www.visualcapitalist.com/sp/anti-satellite-weapons/, retrieved on 15 March 2024.
6. Congressional Research Service (10 August 2021). *Space as a Warfighting Domain: Issues for Congress,* pp. 1-3, https://crsreports.congress.gov/product/pdf/IF/IF11895, retrieved on 27 March 2024.
7. Congressional Research Service (14 November 2022). *Defense Primer: Electronic Warfare*, pp. 1-2, https://crsreports.congress.gov/product/pdf/IF/IF11118/13, retrieved on 27 March 2024.
8. Congressional Research Service (2 January 2024). *Defense Primer: Army Multi-Domain Operations (MDO)*, pp. 1-2, https://crsreports.congress.gov/product/pdf/IF/IF11409, retrieved on 27 March 2024.
9. Croshier, R. (2023). *Handbook for space capability development*, pp. 11-17, 33-48. Center for Global Development, https://www.cgdev.org/publication/handbook-space-capability-development cgdev.org, retrieved on 27 March 2024.
10. Demarest, C. (11 December 2023). *US must dominate in space to win future wars, Marine Corps' Glavysays,* C4ISR net, pp. 1-2, https://www.c4isrnet.com/battlefield-tech/space/2023/12/11/us-must-dominate-in-space-to-win-future-wars-marine-corps-glavy-says/, retrieved on 27 March 2024.
11. Desjardins, J. (4 December 2014). *Space Wars: The Private Sector Strikes Back,* pp. 1-12, https://www.visualcapitalist.com/space-wars-private-sector-strikes-back/, retrieved on 15 March 2024.
12. Euroconsult (2021), https://www.euroconsult-ec.com/press-release/new-satellite-market-forecast-anticipates-1700-satellites-to-be-launched-on-average-per-year-by-2030-as-new-entrants-and-incumbents-increase-their-investment-in-space/, retrieved on 12 May 2024.
13. European Parliament (January 2014). *Space, sovereignty and European security building European capabilities in an advanced institutional framework*, pp. 12-17, https://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/433750/EXPO-SEDE_ET(2014)433750_EN.pdf, retrieved on 27 March 2024.
14. International Relations (2022). *Space and Counter-Space Activities of Great Powers in Outer Space*, vol. 22, no. 2, pp. 397-408, https://cyberleninka.ru/article/n/space-and-counter-space-activities-of-great-powers-in-outer-space/viewer, retrieved on 27 March 2024.

15. Karako, Th. (23 December 2022). *Deterrence, Air Defense, And Munitions Production in A New Missile Age*. Strategika. Hoover Institution, pp. 1-7, 15-34, 36 -43, 62, https://www.hoover.org/research/deterrence-air-defense-and-munitions-production-new-missile-age, retrieved on 15 March 2024.
16. Kunertova, D. (2021). *New Missiles, Eroding Norms. European Options after the Demise of the INF Treaty*. Djøf Publishing in cooperation with The Centre for Military Studies, p. 55, https://cms.polsci.ku.dk/publikationer/nye-missiler-udhulede-normer-europaeisk-sikkerhed-efter-inf-traktatens-ophoer/download-cms-rapport/CMS_Report_2021_4_-_New_missiles_eroding_norms.pdf, retrieved on 15 March 2024.
17. de Leon, J.D. (2021). *Understanding multi-domain operations in NATO*. In *The Three Swords Magazine*, pp. 2-4, https://www.jwc.nato.int/application/files/1516/3281/0425/issue37_21.pdf, retrieved on 27 March 2024.
18. *The Year in Review* (2020). EU Court of Justice, pdf., https://www.google.com/search?client=firefox-b-d&q=%C3%8En+iulie+2020%2C+Amazon+a+primit+aprobarea+de+la+Programul+de+Procedur%C4%83+de+Zbor, EU Court of Justice 2024, retrieved on 12 May 2024.
19. Pixalitycs (5 July 2023). *How many satellites are orbiting the Earth in 2023?*, pp. 1-15, https://www.pixalytics.com/satellites-orbiting-earth-2023/Pixalytics Ltd, retrieved on 27 March 2024.
20. Pope, Ch. (19 April 2023). *Complacency' must be avoided to maintain U.S. superiority in space,* pp. 1-3, https://www.spaceforce.mil/News/Article/3368200/complacency-must-be-avoided-to-maintain-us-superiority-in-space-saltzman-says/, retrieved on 15 March 2024.
21. Science Alert (2023), https://www.sciencealert.com/one-of-the-brightest-things-in-the-night-sky-is-now-a-satellite-launched-in-2022, retrieved on 22 June 2024.
22. Statista (April 2022). *Number of satellites in orbit by major country 2022,* p. 1. Number of satellites in space in 2022, https://www.statista.com/statistics/1343344/orbital-space-launches-global/, retrieved on 27 March 2024.
23. Strategic Studies Institute (14 December 2023). *The need for multi-domain operations,* pp. 17-18, U.S. Army War College, resrep26552.8.pdf, jstor.org, retrieved on 27 March 2024.
24. Taylor Tillman, N. (9 March 2013). *Space Junk: Tracking&Removing Orbital Debris*, pp. 1-5, https://www.space.com/16518-space-junk.html, retrieved on 27 March 2024.
25. The Joint Chiefs of Staff (10 February 2023). *Joint Concept for Competing*, pp. i-ix, 24-29, https://s3.documentcloud.org/documents/23698400/20230213-joint-concept-for-competing-signed.pdf, retrieved on 27 March 2024.

26. Tingley, B. (15 February 2024). *Russian plans for space-based nuclear weapon to target satellites spark concern in US Congress*, pp. 1-2, https://www.space.com/russia-space-nuclear-weapon-us-congress, retrieved on 27 March 2024.
27. Union of Concerned Scientists (1 May 2023). *UCS Satellite Database*, pp. 1-3, Satellite Database: Union of Concerned Scientists, ucsusa.org, retrieved on 27 March 2024.
28. U.S. Army, TRADOC (6 December 2018). *The U.S. Army in Multi-Domain Operations 2028*, pp. i-viii, 5-15, https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf, retrieved on 27 March 2024.
29. U.S. Department of the Army, *FM 3-14, Army Space Operations* (October 2019), pp. v, 1-1-1-11, https://irp.fas.org/doddir/army/fm3_14.pdf, retrieved on 27 March 2024.
30. U.S. Department of the Army, *Joint Publication 3-14, Space Operations* (26 October 2020), pp. i-xii, https://irp.fas.org/doddir/dod/jp3_14.pdf, retrieved on 27 March 2024.
31. U.S. Department of Defense, *Defense Space Strategy Summary* (June 2020), pp. 3-10, https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020_DEFENSE_SPACE_STRATEGY_SUMMARY.PDF, retrieved on 15 March 2024.
32. U.S. Department of Defense (27 October 2022). *National Defense Strategy of United State of America*. In *Missile Defense Review (MDR)*, pp. 1-2/63, https://media.defense.gov /2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF, retrieved on 27 March 2024.
33. Vergun, D. (26 April 2023). *Official Details Space-Based Threats and U.S. Countermeasures,* pp. 1-3, https://www.defense.gov/News/News-Stories/Article/Article/3375577/official-details-space-based-threats-and-us-countermeasures, U.S. Department of Defense: Defense Department News, retrieved on 27 March 2024.
34. Vergun, D. (6 July 2023). *Space.com General Wants Satellites with Sustained Maneuverability.* U.S. Department of Defense, pp. 1-2, U.S. Department of Defense: Defense Department News, https://www.defense.gov/News/News-Stories/Article/Article/3450313/spacecom-general-wants-satellites-with-sustained-maneuverability/, retrieved on 27 March 2024.
35. Visual Capitalist (2024). *Planetary Variables: Quantifying a Changing World,* pp. 1-5*,* https://www.planet.com/products/planetary-variables/, retrieved on 27 March 2024.
36. Wood, T. (20 October 2020). *Visualizing All of Earth's Satellites: Who Owns Our Orbit?*. In *Visual Capitalist*, pp. 1-5, https://www.visualcapitalist.com/visualizing-all-of-earths-satellites/, retrieved on 27 March 2024.

HUMAN BEHAVIOUR IN *"CYBERSOCIETY"* AND ITS IMPLICATIONS FOR NATIONAL SECURITY

Priest Ciprian Ion IONIȚĂ
Romanian Patriarchate
10.55535/RMT.2024.3.8

This study was initiated by the desire to understand to what extent the "virtual adventure" of man in the "cyberspace" is also a form of unconscious search for religion, starting from the very mechanism of functioning of the virtual world, namely by connecting or linking people in a network. Based on this premise, by analysing several scholarly works as well as by investigating the actual behaviour encountered in today's society, we will try to draw out the consequences of the confluence of digitalization and human behaviour and its effects not only on national security but also on geo-political stability at the global level.

Keywords: human behaviour; contemporary religiosity; national security; digitalization; technology; addiction;

INTRODUCTION

Through this study we will try to understand the benefits, but also the risks of *the virtual world* or *cyberspace* for the present man as an individual and as a member of a society. As a starting point, we need to consider the global geopolitical context in which the Internet has emerged and the factors that have fostered the spread of virtual networks. The analysis of the Internet will also include the political, economic and psychological context of mankind in which technology gave birth to the *"Internet"*, as well as the evolution and prospects of this product of technology.

We will often refer to the word *"technology",* but it should be said at the outset that this word can be understood in several ways. Most of the issues raised by technology do not refer to technological advances such as the loom, the thermal or electric motor, the MRI scanner or the F16 airplane, but rather to the digital technologies associated with companies and platforms that develop social networking, *big data*, mobile communications and artificial intelligence technologies, which are increasingly dominant in the social, economic and political life of the world. Therefore, it is very important to understand that a critical assessment of the implications of technological environments is not an aversion to particular technologies such as those listed, and even less a denial of the benefits that technology has achieved over time.

Of course, all technologies, taken as a whole, have helped people to be more informed, expanded human capabilities and created new opportunities, increasing productivity (Bartlett, 2019). However, it does not mean that technology is generally beneficial or that it brings more benefits than risks, because, as new technologies spread, both benefits and risks increase exponentially. Moreover, the instance of technological advancement that we see today is just the beginning, as technologies continue to expand. Therefore, one of the issues that will be analysed in this study is whether or not humanity has control over the trajectory of technological advancement.

All technologies, taken as a whole, have helped people to be more informed, expanded human capabilities and created new opportunities, increasing productivity. However, it does not mean that technology is generally beneficial or that it brings more benefits than risks, because, as new technologies spread, both benefits and risks increase exponentially.

The Internet, as a result of the technological advancement that began in the last century, is defined as a text-based and graphical system of relationships and interactions between individuals (Mitcham, 2005). Through electronic devices, the Internet has become a global network, also referred to as a *"digital habitat"* or *"cyberspace"* (Collins, 1996). The seeds of the Internet emerged in the West at the height of the Cold War in the 1960s, in the context of the confrontation between the two great military powers of the Eastern and the Western worlds, as a counterbalancing reaction to the technological advance achieved by the Soviet bloc with the launch into space of the first satellite – Sputnik. A military project developed by the Pentagon has come to be used on a planetary scale, fundamentally changing life and inter-human relations, opening the way to the age of artificial intelligence, the generation of a new language and a new virtual world. Humankind was in an era of physical and spiritual reconstruction after two world wars and in the midst of the Cold War, during the arms race between the two political-military blocs: West and East. The Internet was a military project of the US Army and we can see it as a success for the West, a weapon that, non-militarily, has conquered the whole world.

A military project developed by the Pentagon has come to be used on a planetary scale, fundamentally changing life and inter-human relations, opening the way to the age of artificial intelligence, the generation of a new language and a new virtual world.

When we are critical of technology, we are referring to the negative aspects that a possible *"cybersociety"* could have. So, we will consider the implications of today's technological system, such as the impersonal automation of the individual, the alienation of personal and community life in favour of a technical organization, and the reduction of the human being to a component part of the global network. What are the vulnerabilities to which we are exposed when technology is present in the most intimate and unexpected places of our lives? To what extent can we even speak of our identity being undermined by the hyper-technization of our lives?

Suffocated by useless information and glued to ubiquitous screens, today's man experiences an artificial, digitized, hectic life devoid of what the fathers of early Christianity called *"wakefulness"* or *"inner calm".* Some researchers have even spoken of a dehumanization of man as a result of his predominant existence in the artificial environment of technology, to the detriment of God-given reality.

This also represents the greatest risk that technology brings, namely the birth of mutations on the specificity of human existence, so that empathy, love, spontaneity and living thought are alienated, and man becomes and is evaluated according to technical criteria, like a machine (Lemeni, 2022).

HUMAN BEHAVIOUR AND NEW TECHNOLOGIES

Media technology, from social networking, media, remote communication to video games, is playing an increasingly important role in people's lives. Thanks to the development of technological systems and the exponential growth in processing power found in increasingly portable devices, people are constantly connected to the internet and the virtual world wherever they are. The existence of these facilities through which people can connect anywhere and anytime with each other creates a conflict between real, face-to-face socialization and pseudo-socialization through online communication platforms.

Thanks to the development of technological systems and the exponential growth in processing power found in increasingly portable devices, people are constantly connected to the internet and the virtual world wherever they are. The existence of these facilities through which people can connect anywhere and anytime with each other creates a conflict between real, face-to-face socialization and pseudo-socialization through online communication platforms.

In terms of the psychological implications that today's technology has, we are living in a unique period in history, characterized by profound changes in human behaviour. The rapid pace of change that is occurring, sometimes without our realizing it, is the effect of the rampant introduction and adoption of technologies in all areas of our lives, and it has fundamentally changed the way we communicate, socialize, work and live. But what are the costs and benefits of using technology in this way for our lives?

While there are some who would argue that the adoption of new technologies in people's lives is a *"win-win situation",* with technology consumers becoming happier and more productive and technology providers enjoying the success of their products, the situation is more complex than at first glance. Although the benefits are obvious, the purpose of this study is to explore whether the claim that the benefits of technology outweigh the risks is true or, if not, what are the risks we face and what is to be done about them? The concerns of sociologists, psychologists and physicians about the effects of technology on human behaviour have been always expressed, but they have often been ignored or even trivialized.

As early as the 19th century, in the *British Medical Journal*, people were warned about a hearing impairment that can occur in people who use the telephone for long periods of time. It is well known that the telephone was the most important invention of the late 19th century, and in a very short time it became a fixture in most homes in the United States of America. Symptoms of that ailment included nervousness, a *"ringing"* in the ear, dizziness, and neuralgic pain (*Church Service by Telephone*, 1904). Also, there are publications of those years that talk about how the telephone affected people's emotional state and behaviour (Marvin, 1988), although at first glance the new invention brought only benefits. The above example emphasizes that new technologies have always raised concerns about their effects on people's health.

How people relate to the latest technological developments and how they have influenced their behaviour in everyday life is an important area of investigation that should be of concern in today's society.

The progress of new technologies tends to make us see the benefits first, ignoring the risks or not seeing them at all. The main danger we run is to see the risks only after the effects are irreparable. How people relate to the latest technological developments and how they have influenced their behaviour in everyday life is an important area of investigation that should be of concern in today's society.

The period in which we find ourselves can be likened to the Enlightenment (1650-1800), when humanity underwent major transformations in terms of consciousness, social behaviour, knowledge and technology. The Enlightenment implied the generation of new freedoms, just as new technologies seem to offer us dizzying and unlimited freedoms. Absolute freedom is a concept of the internet age. But is it also a freedom that corrupts? This feeling of absolute freedom arises due to the fact that the internet is ubiquitous, highly complex and, at the same time, highly attractive to human stimuli at any time and anywhere (Aiken, 2019).

From the year 2000 to 2021, the number of internet users has increased twelvefold (Petrosyan, 2024), with around 5 billion people currently online at any given time. Also, the number of cell phone subscriptions and the hours people spend online is growing exponentially every year. So, we can see that in recent years most people have discovered a new medium in which to spend their time. And just as any move from one real place to another has an effect on the psyche, so human behaviour is affected when we move to a virtual

space, as the environment has a strong influence on us. Therefore, what are the benefits, but more importantly, what are the risks to which we expose ourselves when we step into this realm of virtual sensations and how does it affect the behaviour of individuals in society?

The speed at which we are moving towards a *"cybersociety"* is driven by the usefulness of technology in our lives. The main advantages that media technologies present or the reasons why they are so easily assimilated into our daily activities can be various. Thus, the virtual environment is a source of fulfilment of basic needs such as connecting with loved ones, stimulating positive psychological states of well-being (Guillory, Keilman, Woodruff, Hancock, 2015). Media technology is also a source of effective information, social outreach, entertainment, and a factor of comfort and efficacy, with one of the key purposes of technology being to actually make our lives easier. In a study in which people were asked to describe in one word what they liked most about their smartphone, the most used word was *"convenience"* (Smith, 2012). Today, most people can access the internet from a device carried in their pocket, with the technology giving them instant access

The speed at which we are moving towards a "cybersociety" is driven by the usefulness of technology in our lives.

to a variety of resources that were previously restricted by time and space. Last but not least, while embracing new technologies may mean being prone to certain security vulnerabilities, the same remote communication systems available at the touch of a screen can provide help in the event of an emergency.

Used on a planetary scale, in all areas of human activity, as well as in private life, the internet is a way of life which offers easy access to a virtual network where the speed of connections meets human needs. The fundamental question is to what extent man can control technology and, ultimately, whether man will nevertheless understand what he is looking for by constantly toggling between the real and virtual worlds.

Used on a planetary scale, in all areas of human activity, as well as in private life, the internet is a way of life which offers easy access to a virtual network where the speed of connections meets human needs.

Although the integration of technology in all areas of our lives can provide us with viable solutions to many of our problems, connecting with the virtual environment can disconnect us in a seemingly harmless way from the real world. According to several studies, traditional socializing and connecting with other people face-to-face is closely related to good psychological and emotional well-being (Przybylski, Weinstein, 2012), and connecting with other people through

technology-mediated ways, at the expense of traditional socializing, involves taking real risks, which we will discuss below.

Anyone who has been attracted to cyberspace can testify to the time-distorting effect we are subjected to when we access the online system. Once we enter this space, we risk getting lost in this world, and when we come back, we feel as if we have woken up from a dream. In the real world, the estimation of the passage of time is kept much more effectively than in the virtual world. Many people who use the internet are deceived by the feeling that they are actually in the same place, in the comfort of their own homes, and that nothing has changed since they sat in front of the screen. However, people have honed instincts suited to tangible reality, and in cyberspace they fail in unexpected ways (Aiken, ib.).

Cyberspace presupposes our engagement in multiple tasks at the same time, which results in attention deficits and even limited cognitive functions. It is because we are normally used to focusing on a single task, and the fragmentation of the tasks that our brains have to perform leads to a decrease in the quality of their performance, and this is even more dangerous for young users, as it affects their learning and memorization capacity, so important during school.

Cyberspace is not only an environment that makes it easier for us to perform certain tasks such as sending a message, reading the news or passively watching a programme, but it also hyper-stimulates our brains due to the highly interactive, engaging and highly addictive flow. At the same time, cyberspace presupposes our engagement in multiple tasks at the same time, which results in attention deficits and even limited cognitive functions. It is because we are normally used to focusing on a single task, and the fragmentation of the tasks that our brains have to perform leads to a decrease in the quality of their performance (Liefooghe, Barrouillet, Vandierendonck, Camos, 2008), and this is even more dangerous for young users, as it affects their learning and memorization capacity, so important during school. Moreover, the use of new technologies such as TV and smartphones is linked to concentration and attention deficits (Johnson, Cohen, Kasen, Brook, 2007), and their use before sleep affects sleep quality and the ability to rest (Lanaj, Johnson, Barnes, 2014).

THE *"NEW MAN"* AND THE DIGITAL AGE

How appropriate is the phrase of the writer Virgiliu Gheorghe, describing the situation in the world 15 years ago, referring to the impact that television has had on human behaviour, talking about a *"world enchantment"* through which the *"new man"* was created: *"The new man no longer pursues high ideals; he no longer cares about truth and love, but only about the portion of pleasure and the illusion*

of power that television or the entertainment industry provides him with"! (Gheorghe, 2008).

Although not much time has passed since these assessments, it is not difficult to realize that this project of the *"new man"* is still in progress, and that its evolution has moved in the expected direction, but at an unexpected speed. What is more serious is the fact that, although we can partly predict how man will change, there are also unpredictable aspects, both in terms of how changes will be precipitated and how they will unfold.

In general, when new technological products are invented as a result of technological advancement, they are launched on the commercial market targeting people of a certain age group, as with any product that has a target audience. What is unique about new technologies is their ability to infiltrate all age groups, from children who have not yet learned to speak or write, but are instantly attached to the mobile phone screen, to older people who have become adept at technology faster than expected. This infiltration of media technology into all social and age groups has led to the formation of what we can call the *"new man"*.

What is unique about new technologies is their ability to infiltrate all age groups, from children who have not yet learned to speak or write, but are instantly attached to the mobile phone screen, to older people who have become adept at technology faster than expected.

The specificity of this human evolution is characterized by the limitation of the capacities to interact face to face, people thus becoming less sociable. The new generations are less able to build deep relations with their fellows, to experience or transmit love, affection, and therefore the *"new man"* loses the ability to form lasting relationships, families or communities. And all the above-mentioned aspects represent only the beginning of the transformation that the new generations are undergoing, as the changes that may occur at behavioural, emotional and social levels can have a domino effect. In such a scenario, people could end up living in a society devoid of love and empathy.

Humans are social beings by their very nature, and the desire to connect with others is a fundamental human instinct and even a survival skill. Therefore, any attempt to alter these fundamental abilities and instincts is an attack on human identity and social characteristic. Therefore, yesterday's man is no longer the same as today's man, but not in the sense of the evolution of human civilization, but in the sense of the ontological transformation of man. Today's technology

makes man witness a unique period in history, which we could call an *"evolutionary syncopation"* (Aiken, ib.). Psychologist Mary Aiken is the one who coined this expression, using it in her discourse on the need for face-to-face socialization and the fact that the decline of direct eye contact between people could change the course of human civilization in every respect.

The idea of the *"new man"* is closely related to the fact that, although countless studies have been done on the devastating effects of technology on children, the full effects that will follow are not yet known (Haughton, Aiken, Cheevers, 2015). The repercussions of the use of new technologies by children will only be able to be observed and analysed in depth once the new generations become members of the new society. And if tomorrow's society will be made up of the *"new people"*, the social transformation and implications for national security will be difficult to control or remedy.

The idea of the "new man" is closely related to the fact that, although countless studies have been done on the devastating effects of technology on children, the full effects that will follow are not yet known.

That is why the shape of the society of the future is closely linked to how today's parents will manage the time they spend with their children and the period when they come into contact with the new cyber world. Researchers in the field are unequivocal when they talk about the fact that replacing family time with a tablet, phone or any other electronic device connected to the internet is associated with a range of socio-emotional, physical and cognitive disorders. The speed at which we are moving towards *"cybersociety"* is closely linked to the way we use new technologies, since another risk they present that we have not talked about so far is that the continuous use of digital devices leads to addictions as powerful and dangerous as drug addiction. Any addiction, once established, has a tremendous power to subjugate and transform the human person in a negative way, and a collective addiction on a large scale can have catastrophic consequences for tomorrow's society.

DIGITAL ADDICTION – THE METHOD OF SUBJUGATION

The dependence on technology and the transformation of human society into a *"cybersociety"* seem to be irreversible processes. The fundamentals of human civilization are changing before our eyes and we cannot estimate the impact of the virtual world on the real world, as it is a dynamic, ongoing process. As digital devices have become

indispensable to the homes in which we live, it has been only a matter of time for them to become increasingly portable to the point of becoming a *"digital extension"* of the human being. Although they provide us with convenience, entertainment and portability, these *"digital extensions"*, through their excessive use and connection to the online environment, affect people's behaviour in the sense that they cause addiction, in addition to the other psychological conditions that come along with it (Nazir, Samaha, Griffiths, 2019).

History shows that the term *addictus* has had a very interesting semantic evolution. In the past, the term was used to describe the time for which a slave had to serve his master (Aiken, ib.). Today, by *addiction* we mean a neuropsychological disorder caused by the prolonged and repetitive use of a substance. With the mirage of digital technology, the term *addiction* has broadened its spectrum, in the sense that addiction to digital connection causes the same behavioural effects as other narcotic addictions (Heilig, Mackillop, Martinez, Rehm, Leggio&Vanderschuren, 2021). Also, internet addiction has been shown to be an important predictor of later drug use (Fisoun, Floros, Siomos, Geroulakis&Navridis, 2012).

Imperturbability, productivity and procrastination are much talked about today in the online environment itself, but gaining control and managing the time we spend online are increasingly difficult goals to achieve in a nascent "cybersociety".

Just as a person addicted to drugs struggles with the desire to feed their learned stimulants with certain substances, in the same way, notifications and alerts on a digital device or the compulsive obsession with checking email can cause the internet addict to manifest a drive to constantly check their phone or computer. These impulses that the internet and the virtual world provide are not so different from those produced by slot machines (Aiken, ib.).

Imperturbability, productivity and procrastination are much talked about today in the online environment itself, but gaining control and managing the time we spend online are increasingly difficult goals to achieve in a nascent *"cybersociety"*. There are even apps that can be installed on digital devices to help those who have problems in this area to counteract them.

As cases of internet addiction have increased, studies and surveys have been carried out in many of the countries involved, showing that the number of people with an internet addiction disorder is on the rise, with the most affected age group being adolescence. As far back as the 1990s, David Greenfield, a noted authority in this field, stated

that 10-12% of Americans suffer from Internet addictive behaviour (Greenfield, 1999). Just as drug addiction involves the use of multiple types of narcotic substances, internet addiction encompasses many types of users of the digital space, ranging from those who obsessively check their emails, phone alerts or social network notifications to compulsive shopping sprees, video game playing or pornography addiction.

As shown above, internet technology offers unlimited benefits and possibilities in terms of accessibility and efficiency. Today, through online connection, we can have anything we want delivered to our door or anywhere else, we can instantly contact people thousands of miles away, and just as quickly, we can find information that we once found after hours of searching through libraries. The problem arises when the desire to access the internet grows out of control. The state of today's society provides an enabling environment for it to happen (Aiken, ib.).

Internet technology offers unlimited benefits and possibilities in terms of accessibility and efficiency. Today, through online connection, we can have anything we want delivered to our door or anywhere else, we can instantly contact people thousands of miles away, and just as quickly, we can find information that we once found after hours of searching through libraries.

At the same time, the problems generated by technology addiction continue to evolve and cannot be denied. An interesting claim by those addicted to the internet, which should raise big questions for sociologists and those concerned about the future of society, is that internet deprivation would be the worst thing that could happen to them, far worse than the lack of food, housing, family or relationships.

Among the risks to those who exhibit internet addictive behaviour are psychosomatic disorders such as general malaise, weakened immunity, risk of diseases caused by prolonged exposure to electromagnetic fields caused by digital devices (Zorin, 2014), but also impaired learning and memory, decreased sleep quality, impairment of healthy eating (Yeonsoo, Park, Kim, Jung, Lim&Kim, 2010), locomotor system impairment due to sedentary lifestyle, ophthalmological disorders, mental disorders, socialization impairments (Whang, Lee, Chang, 2003), predisposition to other addictions such as alcohol, tobacco and drugs, and last but not least, deterioration of human spiritual life (Zorin, ib.) as it is replaced by life online. In such circumstances, the Internet unwittingly becomes an idol for man, and compulsive connection to this medium replaces and leaves no room for communication with God, i.e. prayer.

The conditions that an internet addict exhibits largely coincide with those of a psychotropic substances addict. Moreover, in both cases, the effects can even be fatal (Wallace, 2014).

In the case of other types of addiction, abstinence may be the first and most effective method of recovery for the addict, but can the same method be applied to internet addiction? Giving up the internet and technology altogether is not as viable an option as it could only be achieved by total separation from the society in which the new technologies have so deeply infiltrated. In the case of the other types of addiction, eliminating the substances used does not imply such a drastic change in daily habits as would be the case if technology were completely removed from daily life. Today, technology is necessary if we want to work, study, be informed or pay our bills, and therefore the approach to internet-dependent behaviour needs to be rethought. Instead of abstinence, we need to find a way of adapting effectively to the technological environment by becoming aware of its dangers and pitfalls: *"The Internet may be mankind's most seductive and tempting creation"* (Aiken, ib.).

Time has shown us that technology is becoming more and more indispensable to the society members in the years to come, and it is therefore necessary to learn to live with it, but on our own terms. We need to be educated in this realm so that we can become more disciplined and resilient, thereby reducing the chances of compulsive online behaviour.

CONCLUSIONS

In order to adapt effectively and intelligently, we believe that a thorough understanding of how technology affects us is necessary. Time has shown us that technology is becoming more and more indispensable to the society members in the years to come, and it is therefore necessary to learn to live with it, but on our own terms. We need to be educated in this realm so that we can become more disciplined and resilient, thereby reducing the chances of compulsive online behaviour.

When people are subjugated by the virtual world, by altering their ability to relate to others, their identity is also affected and their sense of belonging to a community or a people is diminished. This aspect has direct implications for national security, as it directly targets the way a person shows devotion and love to his or her people, homeland or nation. A high percentage of people addicted to the internet nationwide poses a major risk to the stability of a state, especially in times of national crisis. The strength of a nation and the survival

of a people in history are closely linked to the will of the people to defend their country. Let these important qualities not be undermined by a possible dependence on the virtual environment!

BIBLIOGRAPHY:

1. Aiken, M. (2019). *The Cyber Effect. Psihologia comportamentului uman în mediul online.* București: Editura Niculescu.
2. Bartlett, J. (2019). *Oameni vs. tehnologie. Internetul trebuia să ne elibereze.* București: Editura Nemira.
3. *Church Service by Telephone*. (1904). In *American Telephone Journal,* pp. 65-66.
4. Collins, H.M. (1996). *Interaction without society?: What avatars can't do?* In *Internet Dreams: Archetypes, Myths, and Metaphors* (The MIT Press), pp. 320-321.
5. Fisoun, V., Floros, G., Siomos, K., Geroulakis, D.&Navridis, K. (2012). *Internet Addiction as an Important Predictor* în *Early Detection of Adolescent Drug Use Experience – Implications for Research and Practice.* In *Journal of Addiction Medicine,* vol. 6 (1), pp. 77-84.
6. Gheorghe, V. (2008). *Revrăjirea lumii sau de ce nu mai vrem să ne desprindem de televizor.* București: Editura Prodromos.
7. Greenfield, D.N. (1999). *Virtual Addiction: Help for Netheads, Cyberfreaks, and Those Who Love Them.* Oakland, California: New Harbinger.
8. Guillory, J., Keilman, J., Woodruff C., Hancock J.T. (2015). *Text messaging reduces analgesic requirements during surgery*. In *Pain Medicine*, no. 16 (4), pp. 667-672.
9. Haughton, C., Aiken, M., Cheevers, C. (2015). *Cyber Babies: The Impact of Emerging Technology on the Developing Infant*. In *Psychology Research,* vol. 5, no. 9, pp. 504-518.
10. Heilig, M., Mackillop, J., Martinez, D., Rehm, J., Leggio, L.&Vanderschuren, LJ. (2021). *Addiction as a brain disease revised: why it still matters, and the need for consilience*. In *Neuropsychopharmacology,* no. 46 (10), pp. 1715-1723.
11. Johnson, J.G., Cohen, P., Kasen, S., Brook, S.J. (2007). *Extensive television viewing and the development of attention and learning difficulties during adolescence*. In *Archives of Pediatrics and Adolescent Medicine,* no. 161, pp. 480-486.
12. Lanaj, K., Johnson, E.R., Barnes, M.C. (2014). *Beginning the workday yet already depleted? Consequences of late-night smartphone use and sleep*. In *Organizational Behavior and Human Decision Processes*, no. 124 (1), pp. 11-23.
13. Lemeni, A. (2022). *Tehnicizarea inumană a vieții.* București: Editura Basilica.

14. Liefooghe, B., Barrouillet, P., Vandierendonck A., Camos, V. (2008). *Working memory costs of task switching.* In *Journal of Experimental Psychology: Learning, Memory, and Cognition*, no. 34 (3), pp. 478-494.
15. Marvin, C. (1988). *When old technologies were new: Thinking about electric communication in the late nineteenth century.* New York, NY: Oxford University Press.
16. Mitcham, C. (2005). *Encyclopedia of Science, Technology and Ethics, Farmington Hills.* Editor: Carl Mitcham. MI: Thomson Gale.
17. Nazir, H.S., Samaha, M., Griffiths, D.M. (2019). *The Digital Addiction Scale for Children: Development and Validation*. In *Cyberpsychology, Behavior and Social Networking,* pp. 1-8.
18. Petrosyan, A. (22 May 2024). *Statista.com.*, https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/, retrieved on 15 June 2024.
19. Przybylski, A.K., Weinstein N. (2012). *Can you connect with me now? How the presence of mobile communication technology influences face-to-face conversation quality*. In *Journal of Social and Personal Relationships,* no. 30(3), pp. 237-246.
20. Smith, A. (2012). *The best (and worst) of mobile connectivity.* Washington, D.C.: Pew Research Center.
21. Wallace, P. (2014). *Internet addiction disorder and youth*. *EMBO reports*, no. 15 (1), pp. 12-16.
22. Whang, L.S., Lee, S., Chang, G. (2003). *Internet over-users' psychological profiles: A behavior sampling analysis on Internet addiction.* In *CyberPsychology & Behavior*, no. 6, pp. 143-152.
23. Yeonsoo, K., Park, J., Kim, S., Jung, I.-K., Lim, Y.&Kim, J.-H. (2010). *The effects of Internet addiction on the lifestyle and dietary behavior of Korean adolescents*. In *Nutrition research and practice*, no. 4, pp. 51-57.
24. Zorin, K.V. (2014). *Dependența de computer, de jocuri, de nicotină.* București: Editura Sophia.

A PERSPECTIVE REGARDING THE ADAPTATION *OF ROMANIAN JOINT COMMAND MASTER'S PROGRAMMES* TO THE CURRENT CHALLENGES OF THE OPERATING ENVIRONMENT

Lieutenant Colonel George-Ion TOROI, PhD
"Carol I" National Defence University, Bucharest
10.55535/RMT.2024.3.9

This year marks the 135th anniversary of the establishment of the Higher War College, whose tradition is continued by "Carol I" National Defence University. Over the years, this school has trained many renowned commanders of the Romanian Armed Forces, the relevance of the study programme being ensured by the continuous improvement of the educational process in line with the philosophies of combat and the specificities of armed conflicts.

Today, we are witnessing a profound transformation of our society, which has a direct impact on the way armed forces operate. In an information and digital age that has fundamentally transformed the way of communication, in which the main function of information has changed from knowledge to influence, in an environment where new technologies shape our current way of life and autonomous systems are increasingly present in armed conflicts, military education cannot but keep pace and adapt to these requirements in order to maintain its societal relevance and ensure the timely preparation of the future commanders of the Romanian Armed Forces.

These are the reasons why the article draws the attention of the Romanian military leadership to the need to transform the main university degree programme of its armed forces in order to effectively fulfil the main function for which it was designed, to prepare and provide highly trained personnel capable of assuming leadership positions and actively contributing to the enhancement of the combat power of the Romanian Armed Forces. This study also proposes some directions to be followed in order to increase the relevance of the curriculum in the current operating environment.

Keywords: education; command master's programme; adaptation; generation Z; operating environment;

A.N.: The results of this study are subjective and do not represent the official position of *"Carol I"* National Defence University. I believe that the Ministry of National Defence's competent factors can evaluate the proposals contained in this study, which can serve as a foundation for transforming the joint command master's programmes management.

ROMANIAN MILITARY THINKING

Motto:

"Education is the most powerful weapon which you can use to change the world".

Nelson Mandela

"War is not an affair of chance. A great deal of knowledge, study and meditation is necessary to conduct it well".

Frederick the Great

INTRODUCTION

"Education is the most powerful weapon you can use to change the world", said Nelson Mandela, the politician. Its potential to prepare individuals, to shape characters and perceptions, to transform, even indirectly, the whole of society, makes education an essential tool for the progress of humanity. Education makes a fundamental contribution to the human beings maturing and shaping not only by developing the capacity for critical thinking and analysis with a view to correctly identifying problems, but also by providing the potential for developing innovative solutions to solve them, based on the critical and creative skills acquired through the educational process. School ensures the transmission of knowledge, skills and values (attitudes), all of them being crucial elements in the formation and development of individuals.

Education makes a fundamental contribution to the human beings maturing and shaping not only by developing the capacity for critical thinking and analysis with a view to correctly identifying problems, but also by providing the potential for developing innovative solutions to solve them, based on the critical and creative skills acquired through the educational process.

The military, as an integral part of society, cannot but recognise the importance of education. In the defence system, it is one of the four pillars of training *(figure 1)*, the broad area dedicated to preparing armed forces for planning and successfully conducting military operations.

Training is the second most important military activity for the armed forces after actual combat operations (Army Field Manual Volume 1 Part 7, 2013, p. Foreword). It is a continuous process whose role is to ensure that the military structure is operational to respond to existing

threats. Therefore, education, as a basic component of the Romanian Armed Forces training process, must be carried out in accordance with the strategies and standards of the Ministry of National Defence, constantly reflecting its operational needs. In this regard, military education must be a fundamental pillar of the Romanian Armed Forces transformation.

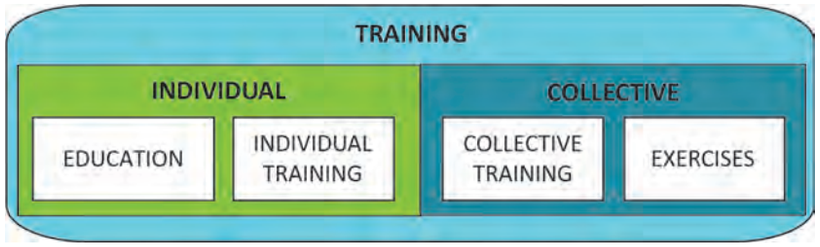


Figure 1: The pillars of force training
(Bi-SCD 075-007 Education and Individual Training Directive, 2015, p. 8)

The evolution of the security environment in the proximity of Romania, the accelerated technologization of all sectors of society, the increased complexity of the current operational environment, the changing character of armed conflicts, as demonstrated by the ongoing one in Ukraine, pose new adaptation challenges for the Romanian military system.

The evolution of the security environment in the proximity of Romania, the accelerated technologization of all sectors of society, the increased complexity of the current operational environment, the changing character of armed conflicts, as demonstrated by the ongoing one in Ukraine, pose new adaptation challenges for the Romanian military system. In this context, military education, as a critical component of this system, must recognise all these elements and take them into account in the planning and implementation of military education, the modernisation of which being also one of the six main lines of action highlighted in the *Romanian Military Strategy* (2021, p. 29).

In this context, the article analyses perhaps the most important education programmes in the career of the Romanian officer, the joint command master's programme, carried out within *"Carol I"* National Defence University. In addition, I have chosen to analyse this form of training based on my six-year experience, two as a Master's student officer and four as an instructor, in the Faculty of Command and Staff, which manages the study programme. Consequently, the results of the study are the product of an empirical approach.

The research problem that I have identified is that the multiple transformations of our society, and implicitly of the operational

environment specific to contemporary conflicts, may contribute to the diminishing relevance of this study programme if it is not adapted correctly and in due time. In addition, we are currently witnessing a generational shift in potential students. Thus, *Generation Z*, the one born between 1996 and 2012 (Dascălu, 2024, p. i), has certain specificities that require a thorough analysis and adaptation of the joint command master's programmes in order to respond effectively to the needs of the beneficiaries and to exploit the specific positive aspects.

The importance of this problem is crucial for the future of the Romanian Armed Forces, given the impact of the command master's programmes on officers' careers. Time is an essential element in this process. I appreciate that now is the right moment to start this analysis, as the results of my research have the potential to contribute to the definition of future directions of adaptation of this study programme. Thus, the recalibration can contribute to maintaining its relevance in the current security environment through the effective preparation of future commanders, considering that Romania has the means and the potential to have an excellent military education system.

The research problem that I have identified is that the multiple transformations of our society, and implicitly of the operational environment specific to contemporary conflicts, may contribute to the diminishing relevance of this study programme if it is not adapted correctly and in due time.

In this context, **the purpose** of the study is twofold. Firstly, to demonstrate the need for a transformation of the university command master's programmes and, secondly, to offer possible directions of evolution, based on a heuristic approach, which will ensure their correct adaptation to the challenges of the current operating environment.

The main target of the study is represented by the decision-makers within the Romanian military system: the study is also addressed to all the academic and auxiliary staff of *"Carol I"* National Defence University, directly or indirectly involved in the educational process carried out within the command master's programmes.

Due to its exploratory nature, **the research methodology** is **qualitative**, attempting to capture in depth the need for adaptation of the analysed study programme. Also, **the reasoning** used is **inductive**, leading to the formulation of the general conclusions, based on the observations and data analysed (Given, 2008, p. 429), in line with the purpose of the study.

In relation to the methodological options presented above, the research is not aimed at validating and testing hypotheses, but is guided by **two main research questions**:

- *What are the arguments for the need to adapt the joint command master's programmes?*
- *How can the joint command master's programmes be adapted to the current challenges of the operating environment?*

In terms of **sampling**, I have chosen to use secondary data to identify the need as well as a possible way to adapt this university degree programme, as their importance in qualitative research is recognised by experts in the field (Birks, 2015, p. 112). Furthermore, in line with this option, the method of **collection** has been document analysis. Also, comparative analysis, a method specific to qualitative research (Given, p. 100), has allowed me to examine similar curricula of some of the Romanian partners in order to identify adaptive solutions based on a heuristic approach.

The structure of the article is modelled on the stated purpose and attempts to provide answers to the two main research questions. Thus, I have first conducted an analysis of the role of the joint command master's programmes in military education and careers, in order to demonstrate the importance of the chosen research topic. Subsequently, I have carried out a study of the main characteristics of the operational environment and their influence on Romanian military education, in order to determine the need for transformation of the study programme under analysis. Finally, I have constructed a design for its adaptation, including possible solutions for four main lines of effort.

THE ROLE OF JOINT COMMAND MASTER'S PROGRAMMES IN MILITARY EDUCATION AND CAREER

"War is not a random aspect of chance. An immense amount of knowledge, study and meditation is required to conduct it well". (Schnaubelt, 2024, p. 16). That is the reason why education is an important component in the development of skills specific to armed conflict, being thus one of the basic pillars of training, as I have already emphasised. Although the latter is recognised in Allied and Romanian

doctrine as central to the realisation of the physical component of combat power, for arguments that are easy to understand I consider that the effects of training have a direct impact on all three components of the combat power of the armed forces (AJP-01, Allied Joint Doctrine, Edition F, Version 1, 2022, p. 49). In addition to developing fighting skills, training can help identify doctrinal areas for improvement, thereby supporting the conceptual component, but it can also provide confidence in combat technique and in one's own forces, achieve group cohesion and build military leaders, all crucial elements of the morale component of combat power.

The role of education, as a component of training, is to provide the skills, knowledge and values that are required by the military in the performance of specific duties, with particular emphasis on communication and thinking skills. At the same time, it enables the military to broaden their horizons by developing a high level of understanding the particular actions and the reasons for their conduct. Friedrich Nietzsche considers that he who understands the purpose of an action will endure any way of solving it. That is why the role of education is crucial, as it complements other forms of training to ensure a deeper understanding of tactical situations and actions. Education also helps to shape individuals and military leaders by creating dilemmas and tactical problems that require them to apply a creative thinking process to develop innovative solutions to the situations created. The ability to operate in uncertain environments and to solve complex problems without pre-defined solutions are also relevant aspects of military education.

The role of education is crucial, as it complements other forms of training to ensure a deeper understanding of tactical situations and actions. Education also helps to shape individuals and military leaders by creating dilemmas and tactical problems that require them to apply a creative thinking process to develop innovative solutions to the situations created.

In the case of Romania, military education is achieved through *"basic courses, career courses, masteral studies, doctoral studies, postgraduate studies and other professional training programmes"* [Order no. M. 30 on 21 March 2012 (updated), 2012, Art. 67)]. The command master's programme is the most important form of training in the Romanian Armed Forces. Its role is to ensure *"the development of the competences necessary for active officers in the exercise of command over formations and units"* (Ib., Art. 73). Moreover, considering that the command-and-control system is the brain of the military organisation, one can observe the impact

of an effective programme on the Romanian military system as a whole. Moreover, the process of development and training specific to officers entails a shift from an emphasis on motor, physical qualities in the early stages of the career to a focus on cognitive skills. I appreciate that the **joint command master's programmes**, which are placed approximately in the middle of the military career, at the earliest in the last two years of the internship in the rank of Captain (Ib., Art. 76), represent **the bridge from the physical to cognitive skills of officers**. That is the reason why it should be emphasised the crucial importance of these programmes in the professional development of Romanian officers.

The process of development and training specific to officers entails a shift from an emphasis on motor, physical qualities in the early stages of the career to a focus on cognitive skills.

If specific procedural knowledge skills are trained in the education system prior to the command master's programmes, this form of training focuses on specific critical thinking skills that ensure a deep understanding of the processes and actions taken, trying to answer questions such as: *"Why is it done in a certain way?", "What are the principles behind these actions?",* and *"How do they fit into a bigger picture to create synergistic effects on the battlefield?"* (Ryan, 2016, p. 49). The *joint command master's* programmes represent the time and place where different branches and specialties understand and deepen their respective roles in combined operations.

ADAPTATION OF THE JOINT COMMAND MASTER'S PROGRAMMES (CM) – *WHY?*

The armed conflict is the most complex, violent, challenging and dynamic human endeavour (MCDP 7 Learning, 2020, pp. 1-3). The above characteristics are naturally transferred to the process of training for this social phenomenon. Societies in general have made considerable efforts to unravel the mysteries of warfare and to adapt their operational procedures and force structures for effective training. Similarly, understanding the characteristics of the nature and character of war has always been one of the preoccupations of the armed forces.

The first prerequisite for any transformation, however, is an awareness of the need for it. To this end, the present section is devoted to identifying and presenting the main factors in relation to which

I believe such adaptation is necessary. For an effective presentation, I have divided them into two broad categories:

- the features of the current operating environment, including elements specific to the nature of contemporary conflicts;
- the characteristics of the human resources to be admitted to the command master's programmes.

Features of the current operating environment

Increased competition between major actors with diverging interests is driving the evolution of today's society towards a multipolar world (Strategic Survey 2022. The Annual Assessment of Geopolitics, 2023, p. 27). **The struggle for global power and dominance** has become increasingly fierce in recent years. In addition, the unprecedented technological developments and the characteristics of the digital and information age in which we live have contributed to the **increased complexity of the current operating environment**. A modern-day paradox is that, although intelligence gathering systems have evolved enormously, the **uncertainty specific to armed conflict is greater than ever**. In this context, **military education needs to redefine its objectives** from the area of delivering knowledge to that of training the military's ability to think critically, to understand and solve unfamiliar problems, and to operate effectively in this uncertain environment.

The struggle for global power and dominance has become increasingly fierce in recent years. In addition, the unprecedented technological developments and the characteristics of the digital and information age in which we live have contributed to the increased complexity of the current operating environment.

Armed conflicts have been an integral part of history since ancient times (Palazzo, 2023, p. 9). They have entailed, in addition to elements that have remained constant in the face of the passage of time, certain evolutionary features. They were part of the character of conflicts. The preparation of armed forces is dependent on a correct understanding of these characteristics. In the following, I will highlight the **main features specific to the character of contemporary conflicts and the way in which they might influence the military education process.**

Mental focus on large-scale combat operations

Recently, we have witnessed a shift in the conflict paradigm from counter-insurgency operations, typical to the beginning of this century, to large-scale combat operations (Nistorescu, 2022, pp. 2-3). This shift is taking place against the backdrop of the trend towards a multipolar

society and the intensification of the global competition for power and influence among the major players, as I have outlined above. We are also witnessing an acceleration in the rearmament and training of armed forces, which underlines the importance of finding effective solutions in military education as well.

Humans, not machines, will continue to be at the centre of the armed conflict

Even though the technological developments we are witnessing today are fundamentally shaping the way we live, I consider that people, not machines, will continue to be the central element in armed conflicts. It is expected, even though technology has evolved enormously, that the human dimension will remain a fundamental feature in the way wars are fought. In this regard, the level of training, experience, education, character, morale and cognition will continue to remain critical elements in the way conflicts evolve. Although technology has shaped many of the processes specific to the military domain, the ability to correctly identify not only the operational problems but also the solutions to them, including the decision-making process will remain specific to the human dimension. That is the reason why the human resource education will continue to remain a very important factor in the armed forces training.

The ability of armed forces to correctly understand the operational situation and to develop plans that maximise the use of capabilities while exploiting the enemy's vulnerabilities can be the precondition for operational success in today's military conflicts.

The importance of tactical and operational levels of war and the synchronisation of actions and effects between them in all domains of operations

The ability of armed forces to correctly understand the operational situation and to develop plans that maximise the use of capabilities while exploiting the enemy's vulnerabilities can be the precondition for operational success in today's military conflicts. There is an increasing need to synchronise the actions of all the armed forces services in order to achieve convergent effects across all operational domains, which is specific to multi-domain operations. Therefore, understanding how each weapon and service is used operationally and how they interact to enhance their mutual effectiveness is a critical element of contemporary conflicts. It requires a focus on how operations are conducted at both tactical and operational levels, which must also be part of the curricula of each specific institution.

The morale component is highly relevant in the current context

Morale is *"an affective state, a temporary state of mind, a temporary disposition of the soul, relating to strength, desire, firmness to endure danger, fatigue, hardship".* (*DEX Online*, 2024) It plays a crucial role in any armed conflict. In the same vein, leadership is a morale multiplier for troops. The ongoing conflict in Ukraine has demonstrated the positive influence of leaders on countless occasions. That is the reason why the theoretical deepening of the concept of leadership as well as the development of leadership skills must be among the priorities of military education. It is clear that modern military operations require leaders who are competent at both tactical and operational levels.

The importance of information in the information environment

Rapid and unprecedented developments in information technology have enabled a level of connectivity and access to knowledge unimaginable just a few years ago. As a result, accurate information has become a vital resource for any warfighter in today's confrontational environment. Shaping the narrative of actions to influence different audiences has become a central element in the quest for information superiority over the adversary. Given the characteristics of the current information environment, influence operations have gained a privileged place in the operational concepts of most relevant actors.

Technologization of the battlefield

The ability to make decisions faster and more accurately than the enemy, coupled with the development of long-range weapons and the reduction of time to target, are key advantages of the modern battlefield. Today's technology has had a direct impact on all branches of the military. Whether it is the process of targeting and engagement, intelligence gathering and analysis, or communications and sustaining the operational picture, technology has transformed the way the armed forces operate. In this context, there is a need for training that takes into account the impact of technology on the art of warfare. Technological developments also offer new avenues and tools for education, such as simulation systems, which educational institutions must integrate into the academic process.

Today's technology has had a direct impact on all branches of the military. Whether it is the process of targeting and engagement, intelligence gathering and analysis, or communications and sustaining the operational picture, technology has transformed the way the armed forces operate.

Specific human resource traits

The adaptation of the command master's programmes should also take place in the context of a change in potential students. The next generation, **Generation Z**, recognised as having different characteristics from the previous ones, is imposing a new approach to education, in general, and to military education, in particular (Cilliers, 2017, p. 188). Each generation brings with it particular aspects that are shaped by the social, technological or political context, by events and trends specific to a certain period. All this leads to differences between generations in terms of how they relate to the world, their value system, their opinions and attitudes, and their behaviour. (Dascălu, ib.).

Having lived in a highly developed era in terms of access to technology, Generation Z is highly tech-savvy, deeply engaged in social networks and the internet, and willing to voice their opinions and challenge existing norms. This generation has grown up in a digital environment, being the first to have access to the internet and technology from an early age. The use of social networks is an integral part of their daily lives, with the potential risk of influencing their opinions, as well as their behaviour and even their career choices. All these characteristics pose a number of challenges for the education system. There is much interest in the academic field in understanding the specific characteristics of how individuals learn, in order to optimise and adapt the learning process in relation to the specific characteristics of each generation, in order to meet societal needs (Hernandez-de-Menendez, 2020; Cilliers, 2017; Dolot, 2018; Kuleto et al., 2021). In this context, I appreciate that the Romanian military education should be aware of these generational changes and take measures to streamline the academic process.

Adaptation is a prerequisite for the survival of any entity. The coherence between existing doctrines, the specific characteristics of today's conflicts and the specific analytical programmes of different military education curricula ensures relevance and coherence in the process of force training.

ADAPTATION OF THE JOINT COMMAND MASTER'S PROGRAMMES (CM) – *HOW?*

NATO considers that, *"to maintain military superiority and prevail in future conflicts, Alliance forces must constantly adapt, evolve and innovate"* (Framework for Future Alliance Operations, 2018, p. 22). Adaptation is a prerequisite for the survival of any entity. The coherence between existing doctrines, the specific characteristics of today's conflicts and the specific analytical programmes of different military education curricula ensures relevance and coherence in the process of force training. Training, and therefore education, cannot remain passive in the face of the new challenges of today's society, in general, and of the operational environment specific to today's conflicts, in particular. Identifying the need for change and developing viable solutions for the development of military education represent integral parts of the adaptation process. It requires a high degree of flexibility, vision and willingness to improve in order to adapt the educational process and maintain its relevance within the military organisation.

As the main form of training in the Romanian Armed Forces, the joint command master's programme requires a comprehensive approach to adaptation. This transformation can only be achieved within a broader adaptation of the entire Romanian military education system. There must be a synchronisation of the competences imparted during each form of training, which implicitly requires a correlation with the level of potential functions that future graduates will be able to perform.

As the main form of training in the Romanian Armed Forces, the joint command master's programme requires a comprehensive approach to adaptation. This transformation can only be achieved within a broader adaptation of the entire Romanian military education system.

However, the analysis proposed in this article focuses only on the command master's programmes, because I consider that the process of transforming all military education should begin with this degree, given its importance and weight in the knowledge of officers. Subsequently, all other forms of training in Romanian military educational institutions can be modelled on them.

Certainly, the ways in which the command master's programmes can be adapted may vary in relation to the person conducting the analysis. Elements such as military experience, teaching experience, level of familiarity with the curriculum, level of understanding of how the curriculum is currently delivered, as well as the level of understanding of the nature of contemporary conflicts and the characteristics of the operational environment, are elements in relation to which differences in approach may arise.

I have chosen elements of operational design as a way of presenting the adaptation process specific to this programme *(figure 2)*. I have identified a desired end state and four Lines of Effort (LoE), which I will describe in the following sections.

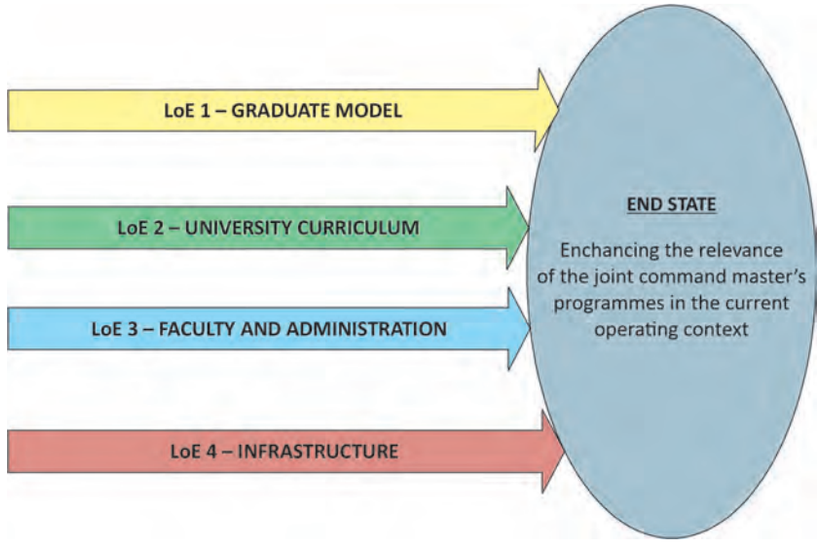


Figure 2: The adaptation of the joint command master's programmes (author's design)

Excellence is an ongoing process and I therefore recognise the importance of continuing the positive elements that have laid the foundations for the extended tradition of the Master of Arts in Interagency Leadership. My proposed design therefore incorporates elements that have already been implemented in this programme and have proved their worth. **The product thus represents a marriage of tradition and innovation**, both aimed at enhancing the relevance of the command master's programmes in today's security environment.

The following four sections describe specific elements of the four strands. I have opted for a tabular presentation in order to ensure that the proposals presented are as accurate and easy to understand as possible.

LoE 1 – Graduate Model

Master's students are the most important image vector of *"Carol I"* National Defence University. Their importance is crucial in the educational process of the command master's programmes. Understanding the specific elements related to age, level of experience, social aspects should be integrated into the way of organising the educational process. In addition, curricula must reflect elements specific to the nature of today's conflicts and operating environment.

Central to this is the graduate model. It represents a requirement of the beneficiary on how the product of the command master's programmes should look like in order to be useful to the Romanian Armed Forces after graduation.

In *table 1*, I have highlighted the main student-specific aspects in order to adapt the Master's programme to the specific challenges of the current operational environment.

Table 1: Proposals on the adaptation of the Master's degree programme in joint command from the graduate model perspective (author's design)

GRADUATE MODEL	
1.	**GRADUATE MODEL**
	• The graduate model is the concept around which the curriculum and duration of the programme are modelled. In essence, it reflects what the beneficiary wants a potential graduate to look like. • In constructing this model, the three domains of learning – **Knowledge** (knowing), **Skills** (doing) and **Attitudes/Values** (being) – should be taken into account.
2.	**DEVELOP MILITARY SKILLS FOR THE TACTICAL AND OPERATIONAL LEVELS OF COMBAT**
	• The ability to understand and operate with concepts specific to both tactical and operational levels of operations ensures that officers are best prepared to meet the challenges of today's operational environment. • The importance of the tactical and operational levels, and the synchronization of actions and effects between them in all areas of operations drive this educational need.
3.	**LEADERSHIP TRAINING**
	• Leadership is an essential component of organisational development and a critical aspect of the morale component of combat power. • Leadership is recognised as one of the most important components in the military education process. (Scipanov, 2023, p. 137). • Developing **adaptive leadership** skills (MCDC Future Leadership, 2020, p. 3). • Developing **self-confidence** for all students. • Cultivating **team spirit**. • Developing **positive character traits**: integrity, responsibility, control, mental flexibility, discipline, emotional intelligence, empathy, perseverance etc.

GRADUATE MODEL	
4.	**DEVELOPING CREATIVE AND CRITICAL THINKING**
	• Building an **adaptive mindset** based on flexible and innovative thinking. (Scipanov, ib.) • Developing **skills to operate in uncertain environments**, identifying root causes of problems and developing creative solutions to solve them. • Understanding one's own **cognitive limitations (biases)** that may influence decision making. • Developing skills to **solve uncertain problems** rather than understanding a **pre-defined formula** that may create **extended vulnerabilities.**
5.	**DEVELOPING COMMUNICATION SKILLS**
	• **Communication is essential in all military-specific activities.** (Scipanov, ib.). It ensures effective and clear communication of the commander's vision for solving the operational problem, sets the stage for successful negotiations, and motivates subordinates in critical situations.
6.	**DEVELOPING DIGITAL COMPETENCES**
	• In the digital age in which we live, the **inability to operate military domain information systems and software can lead to increased vulnerability.** • In today's highly volatile environment, gaining the decision advantage over the adversary by accelerating the **decision-action cycle** (OODA – Observe, Orient, Decide, Act) can also be achieved by maximising the use of various specialised technologies and software to support the **critical functions of military operations**, such as: – providing COP (Common Operational Picture) – providing SITAWARE (Situational awareness) – operational planning – decision making; – targeting and engaging by supporting the targeting process; – logistic support planning; – providing electronic communications etc. • An example is the development of skills to understand and operate **FAS**s (Functional Area Services).

LoE 2 – University Curriculum

A university curriculum is a set of subjects and educational content. It can include course structure, educational objectives and teaching and assessment methods. It is derived from the graduate model and represents a transcription of the competences to be trained into study subjects. In *table 2*, I have highlighted the main proposals that I consider appropriate to maintain the relevance of the Master's degree in the current environment. I also emphasise that some of these elements have already been reflected in the academic curriculum and only require some adjustment.

Table 2: Proposals for the adaptation of the curriculum of the joint command master's programmes (author's design)

UNIVERSITY CURRICULUM	
1.	**NATURE OF INFORMATION**
	• **Study both the tactical and operational levels of combat.** • The analytical programme specific to the command master's programmes should include the transmission of knowledge and the training of skills specific to **tactical and operational level** structures. • It should be correlated with the level of information provided in the other continuous training programmes. • In order to understand the **close fight**, it is necessary to study **Brigade-** (similar-) level operations. The operational relevance demonstrated in the Russian-Ukrainian conflict, the force structure of the Romanian Armed Forces, the potential functions that will be filled after graduation determine the need to study this hierarchical level in depth. • Studying **brigade** level also provides a solid knowledge base without which it is impossible to study the other higher levels in depth. • Deep fight requires the study of the tactical echelons of **Division and Warfighting Corps** (WFC) or equivalent. The similarity of the combat modes of these two echelons makes it possible to study them simultaneously. In the study programme dedicated to these two types of structures, specific elements must be taken into account in order to fulfil the three specific functions of their combat: in-depth combat, support for contact combat and protection of the rear. • **LCC/MCC/ACC –** How to organize and conduct the operations of the component commands of the force services. • **Combined Forces Command** – provides operational-level knowledge on how to plan and conduct a major operation or campaign.

UNIVERSITY CURRICULUM	
2.	**CURRICULUM**
	• Adjust curriculum to reflect the specific operational needs of the current operating environment as well as the specific challenges and features of current conflicts. In this regard, I appreciate the following information as absolutely mandatory for the adaptation of the command master programs: – **Tactical level operations planning** – brigade, division, combat corps (WFC), LCC/similar. – **Operational level operations planning** – Combined Forces Command. – **Cognitive limitations in decision making.** – **MDO** – Multi-Domain Operations. – **Hybrid Warfare.** – **Risk Management.** – **Battlespace Management** (BM). – Operation preparation – e.g. **rehearsals**. – **Operations execution** (rapid decision-making process, battlefield organisation of command, battle tempo, KM process, targeting process, JISR process etc.). – Activities specific to the **battle rhythm**: CUB (Commander's Update Brief), BUB, INTEL WG/Board, IO WG/Board, Assessment WG/Board, TGT WG/Board, DASM – synchronisation of the operation. – **Preparation of specific documents** – OPLAN/OPORD, FRAGO, WARNO etc. – **Reporting system** (R2 – Reports and Returns) – Daily SITREP, INTREP, INTSUM etc. – **Military Intelligence** – IPB, JIPOE and CUOE processes, IRM&CM, JISR, multi-source information processing and analysis methods, I&W (Indicators and Warning) system. – **Information operations** – Information Environment Assessment (IEA) process, information operations planning, deception and countermeasures, OPSEC (Operation Security), PSYOPS, CIMIC etc. – **Analysis of potential adversaries** – organisation, equipment, tactics and procedures. – **Leadership** – it is essential to instil specific values in order to train future military leaders. – **Military art history** and **military geography.** – **Geopolitics** and **Geostrategy** (Security Studies). – **English.**

UNIVERSITY CURRICULUM	
3.	**DURATION OF THE STUDY PROGRAMMES**
	• The length of the programme should be **proportionate to the amount of information to be conveyed** during the CM. • Given the information I have presented in the first two points, I consider that a duration of **2 years – 120 credits** would ensure the viability of the programme. • In the first two semesters, the tactical level specific to the armed forces structures will be studied in order to respond to their needs, with semesters 3 and 4 focusing on joint level operations. Such an approach, I believe, best meets the need to prepare officers for this form of education. • Although it may seem a long time, the long-term benefits will surely outweigh the investment, given that the **Master's degree provides the overwhelming theoretical foundation for the remainder of the military careers**. • I also note that this duration is successfully practised in similar programmes in other partner countries.
4.	**MULTINATIONALITY OF THE STUDY PROGRAMMES**
	• To ensure the relevance of the undergraduate programme, it may also include a multinational component. In this respect, I envisage two lines of action. • Organisation and implementation of **exercises with international participation** from other similar universities with a similar profile of some of the Romanian partners. • Organisation of a **Master's format in English**, in which students from Romania's partner countries can also participate. • I appreciate that such an option would contribute to **increasing the relevance of Romania's position as a regional security pole**.
5.	**CONTINUOUS ADAPTATION OF THE STUDY PROGRAMMES**
	• Conduct an **institutionalised process of feedback** from the Master's students, but also from the force services as the main beneficiaries of the product. • Continuous assessment of changes in the operational environment and armed forces services specific concepts to ensure the operational relevance of the programme. In this respect, a **much closer relationship with the beneficiary** would be conducive to the improvement of the Master's programme.

LoE 3 – Faculty and Administration

Teaching is a noble art and this statement underlines the importance and value of the act of delivering knowledge in the command master's programmes. Teaching is more than just imparting knowledge. The role of the faculty is also to build character, to inspire students, and to contribute directly to their formation as competent, highly critical and capable future commanders and staff officers. However, teaching cannot function effectively without a properly sized and well-trained administrative apparatus. *Table 3* highlights the key elements specific to the faculty that should be considered in the command master's programmes.

Table 3: Proposals on the adaptation of the joint command master's programmes from the perspective of the faculty and administration (author's design)

FACULTY AND ADMINISTRATION	
1.	**INSTITUTIONALIZED ACADEMIC TRAINING**
	• An essential prerequisite for the educational process is a **well-trained and experienced academic staff**. This must be a priority for the military institution. • For this reason, I personally believe that the young members of the academic staff, because of the subsequent influence they can have and the potential effects they can create in the future, should be part of a **priority** programme of **participation in the main courses abroad** relevant to their position. • Moreover, their **participation as observers in the main training events** of the Romanian Armed Forces can contribute significantly to their professional development.
2.	**PROFESSIONAL ETHOS**
	• **Professional ethos** in education is a **set of values, norms, principles and behaviours** that govern the work and conduct of the academic staff. Strict adherence to it will result in the behaviour of future commanders being modelled. • **The teacher – a role model for master's officers**. It will contribute to the training of future commanders, but also to the maintenance of a relationship that will continue after the completion of the studies, ensuring the possibility of sharing experiences in the future. • **Characteristics required for teachers** (MCDP 7 Learning, 2020, pp. 3-16; Dascălu, p. 26): professionalism; selflessness; fairness; respect; communication skills; ability to inspire by personal example; empathy; leadership and mentoring.
3.	**CONTINUOUS IMPROVEMENT**
	• **The relevance of the teaching authority at this level can only be maintained by maintaining a high and updated level of expertise** and by identifying appropriate methods to create the optimal learning environment for the Master's officers. It implies the need for the academic staff continuous professional development. • This continuous training would also have the **potential to inspire future students**, as it is known that one of the characteristics of Generation Z is that they feel motivated by teachers who are eager to evolve (Dascălu, ib.). • It is also important to **facilitate teachers' access** to relevant national and especially international information from **NATO networks.**
4.	**CREATING THE OPTIMAL LEARNING ENVIRONMENT**
	• The first step in **setting up an optimal framework** is to determine the level of knowledge of those responsible for the training, and then to present the information in such a way as to ensure that it is optimally absorbed by them and that the training objectives are achieved. • Approach the **teacher-student relationship** with a **high degree of mutual respect.** • Modelling lessons to **stimulate students' creative and critical thinking.** • **The use of Wargaming** (WG) **in the educational process** (Dascălu, p. 20). It is recognised that WG is an undervalued tool in the educational process. There is a growing interest in similar military higher education programmes to use this tool in the educational process (Sullivan, 2020; Ruhnke, 2020; Bartels, 2020). • **The use of vignette-based situations to develop critical thinking skills in officers to identify optimal solutions to the problem at hand.** • **Force-on-force training** has been shown to be a beneficial interactive experience and knowledge-building framework for students (Haydock, 2023; Mankowski, 2017). Making decisions and adapting in the face of a real adversary who is also carrying out the same activities can simulate elements specific to the nature of conflict that are otherwise difficult to replicate, such as uncertainty or friction, thus supporting the training of officers. • **Interactive organisation of the lessons**, involving the trainee officers in the way they are conducted. Use of NATO methods to provide a framework for problem solving. (The NATO Alternative Analysis Handbook, 2017, pp. 17-117).

	FACULTY AND ADMINISTRATION
	• **Encourage constructive discussions** during class time. • Provide continuous and accurate **feedback** on the Master's officers training path to ensure the framework for their adaptation. • **Invite experienced military professionals** to teach to ensure the correlation between theory and practice.
5.	**TEACHER SELECTION AND STAFFING**
	• The recruitment of teaching staff must be one of the Ministry of Defence's **employment priorities**. • **Create conditions for attracting and retaining the best officers** in the ranks of the teaching staff, emphasising experience, willingness, level of knowledge and character.
6.	**DEVELOPING THE MENTORING PROGRAMME FOR YOUNG INSTRUCTORS**
	• **The training of new instructors** from the instructor corps must be a mandatory condition for the Romanian military education system. • In this sense, the implementation of a mentoring programme for young instructors **can contribute significantly to their professional training.** • Such a programme can also provide a **positive and beneficial framework for directed learning.**
7.	**CAREER DEVELOPMENT IN TEACHING**
	• The conditions for a young teacher to develop a teaching career require a considerable effort in the area of research. • Although research has a beneficial role to play in the process of teacher maturation, I appreciate that a **greater focus on teaching activities in career development** could be much more beneficial to the teaching process. • This proposal is related to an earlier one, specific to the academic curriculum, on the establishment of a department dedicated exclusively to conflict research at tactical and operational levels.
8.	**ESTABLISHMENT OF A CONFLICT RESEARCH DEPARTMENT AT TACTICAL AND OPERATIONAL LEVELS**
	• Research is essential for development and innovation. • Such a decision would have several **positive effects:** – Firstly, it would relieve faculty from the research component and **ensure a better focus on the teaching component.**

	FACULTY AND ADMINISTRATION
	– Secondly, it would provide the framework for **identifying trends in the evolution of conflicts** and could provide valuable information for **adapting Romanian military doctrines** and, indirectly, military education. – Thirdly, the possibility of staffing this department with **Romanian military reservists with extensive experience**, so that the military system can benefit from the knowledge they have acquired during their careers.
9.	**DEVELOPMENT OF ADMINISTRATIVE STAFF WITHIN THE FACULTIES**
	• Certainly, the functionality of the study programme cannot be achieved without a **well-prepared and sized administrative apparatus.** • Such a measure would ensure that the **teachers would be relieved of administrative tasks** and their efforts would be directed to the preparation of teaching activities, which is their essential function.

LoE 4 – Infrastructure

Investment in infrastructure completes the framework for adapting the command master's programmes. Without a modern infrastructure, properly sized in relation to the needs and the number of students, the fulfilment of the crucial conditions specific to the other three lines of effort will not have the expected effects. The infrastructure must therefore enable realistic and effective practical training to prepare officers for complex and unpredictable scenarios. *Table* 4 highlights some important elements related to infrastructure development as a critical requirement for curriculum adaptation.

Table 4: Proposals on the adaptation of the command master's programmes from the infrastructure perspective (author's design)

	INFRASTRUCTURE
1.	**DIGITALIZATION**
	• Development of **digital libraries** with easy access to documents in electronic format. • Use of **FAS**s (Functional Area Services) in the learning process. • Use of **virtual reality systems** to support situational understanding and decision making (e.g. systems that can design the battle space in 3D and automatically calculate possible mobility corridors or blind zones etc.).

INFRASTRUCTURE	
2.	**EDUCATION COMMAND POSTS**
	• Organisation of replicas of command posts for all hierarchical levels studied for CM. • These **command posts should be organised and technologically equipped similarly to the real ones of the Romanian armed force structures.** It would ensure the fulfilment of one of the training principles: *"Train as you will fight!".* • Possibility to connect the Command Posts to the **JCATS** type simulation systems already existing in *"Carol I"* National Defence University.
3.	**MWR (MORALE, WELFARE AND RECREATION) FACILITIES – OFFICERS CLUB**
	• As in combat, people need breaks and disconnection to function optimally and perform at their best. • The organisation of an **Officers' Club** could provide moral support to Master's officers during their studies.

The main research question addressed in this article is whether the military education, in general, and the command master's programmes, in particular, should adapt to the challenges of the current operating environment and streamline the training of Romanian master's student officers from this form of training.

CONCLUSIONS

The multiple transformations of the current operating environment, as well as the main characteristics of the society in which we live, overwhelmingly influence the way military education should be conducted. The main research question addressed in this article is whether the military education, in general, and the command master's programmes, in particular, should adapt to the challenges of the current operating environment and streamline the training of Romanian master's student officers from this form of training.

In this respect, the study is aimed to ensure the fulfilment of two main objectives. Firstly, to sensitise the main decision makers in the Romanian Armed Forces to the need to adapt the command master's programmes, and secondly, to provide a practical product for the transformation of this study programme.

The main outcome is a design consisting of four broad areas of effort: the academic curriculum, the faculty, the master's officer corps and the infrastructure. I appreciate that it can provide an effective framework for the adaptation of the command master's programmes, providing the prerequisites for high quality military education.

The recalibration of this programme can have multiple benefits. The most important of them is to maintain the relevance of the master's programme in the new operational environment, thus continuing its long tradition. In addition, to attract personnel to this form of training and to enhance the combat capability of the Romanian Armed Forces by preparing future leaders capable of responding effectively to contemporary challenges, the *raison d'être* of the command master's programmes.

I am aware that the **process will not be easy.** It will require a **huge collaborative effort** from everyone involved in the change: academic staff, students, support staff. However, with effective communication, continuous monitoring and adaptation, I am confident that **it can be achieved**. We must not forget that the sooner we start, the sooner the effects will have a positive impact on the Romanian military system. That is the reason why I would like to conclude with an exhortation, which is also the motto of *"Carol I"* National Defence University: *"Labor improbus omnia vincit!".*

BIBLIOGRAPHY:

1. *AJP-01. Allied Joint Doctrine, Edition F, Version 1.* (2022). NATO Standardization Office.
2. *Army Field Manual,* Volume 1 Part 7 (2013). UK: Ministry of Defence.
3. Bartels, E.M. (2020). *Wargames as an Educational Tool*, The Forge: https://theforge.defence.gov.au/wargaming/wargames-educational-tool, retrieved on 12 May 2024.
4. *Bi-SCD 075-007 Education and Individual Training Directive* (2015). NATO BI-STRATEGIC COMMAND.
5. Birks, M., Mills, J. (2015). *Grounded Theory: A Practical Guide.* 2nd edition. London: Sage Publications.
6. Scipanov, L.V., Bodescu, A. (2023). *Higher military education focused on quantifiable learning outcome*s. In *Bulletin of "Carol I" National Defence University* (1), pp, 132-142, https://revista.unap.ro/index.php/bulletin/article/view/1686/1691, retrieved on 21 May 2024.
7. Cilliers, E.J. (2017). *The challenge of teaching generation Z. PEOPLE International Journal of Social Sciences,* Volume 3 Issue 1, pp. 188-198.
8. Dascălu, D.T. (2024). *Generation Z and Joint Professional Military Education: Final Synthesis Report.* Santa Monica. California: RAND Corporation, https://www.rand.org/pubs/research_reports/RRA3249-1.html, retrieved on 17 May 2024.
9. *DEX Online* (2024), https://dexonline.ro/definitie/moral, retrieved on 13 May 2024.

10. Dolot, A. (2018). *The characteristics of Generation* Z. *E-mentor, 74(2)*, pp. 44-50.
11. *Framework for Future Alliance Operations.* (2018). Norfolk: NATO Allied Command Transformation.
12. Given, L.M. (2008). *The SAGE Encyclopedia of Qualitative Research Methods,* vol. 1&2. California: Sage Publications.
13. Haydock, T. (2023), US Army Maneuver Center of Excellence, https://www.moore.army.mil/infanTry/Magazine/issues/2023/Winter/PDF/10_Haydock_txt.pdf, retrieved on 12 May 2024.
14. Hernandez-de-Menendez, M., Escobar, C.A., Morales-Menendez, R. (2020). *Educational experiences with Generation Z*. In *International Journal on Interactive Design and Manufacturing (IJIDeM),* vol. 14, pp. 847-859, https://www.researchgate.net/publication/343356700_Educational_experiences_with_Generation_Z, retrieved on 12 May 2024.
15. Kuleto, V., Ilić, M.P., Stănescu, M., Ranković, M. (2021). *Extended reality in higher education, a responsible innovation approach for generation Y and generation Z*. *Sustainability,* 13(21).
16. Mankowski, M. (2017). *Putting the Human Adversary into Professional Military Education*, The Cove: https://cove.army.gov.au/article/putting-human-adversary-professional-military-education, retrieved on 12 May 2024.
17. *MCDC Future Leadership* (2020). Multinational Capability Development Campaign.
18. *MCDP 7 Learning* (2020). Washington D.C.: US Department of the Navy.
19. Nistorescu, C.V. (2022). *Războiul din Ucraina și implicațiile lui asupra modului de abordare a operațiilor de luptă în domeniul terestru*. *Colocviu strategic* (206.12), pp. 1-9.
20. *Order no. M. 30 on 21 March 2012 (updated)* (2012)/*Ordin nr. M. 30 din 21 martie 2012 (actualizat) pentru aprobarea Instrucţiunilor privind recrutarea, selecţia, formarea profesională şi evoluţia în cariera militară în Armata României*. Ministerul Apărării Naționale, https://lege5.ro/Gratuit/gmytimrqgu/ordinul-nr-30-2012-pentru-aprobarea-instructiunilor-privind-formarea-profesionala-si-evolutia-in-cariera-militara-in-armata-romaniei, retrieved on 17 May 2024.
21. Palazzo, A. (2023). *Land Warfare: An Introduction for Soldiers, Sailors, Aviators and Defence Civilians*. In *Australian Army Occasional Paper,* no. 14.
22. Ruhnke, V. (2020). *Games as a Window on a Complex World*, The Forge: https://theforge.defence.gov.au/wargaming/games-window-complex-world, retrieved on 21 May 2024.
23. Ryan, M. (2016). *The Ryan Review. A study of Army's education, training and doctrine needs for the future.* The Australian Army.
24. Schnaubelt, C.M. (2024). *How to write a strategy.* Rome: NATO Defense College.
25. *Romanian Military Strategy/Strategia Militară a României. Capacitate defensivă credibilă, pentru o Românie sigură, într-o lume marcată de noi provocări* (2021). București: Ministerul Apărării Naționale.
26. *Strategic Survey 2022. The Annual Assessment of Geopolitics* (2023). London: The International Institute for Strategic Studies. Routledge.
27. Sullivan, I. (2020). *Would You Like to Play a Game? Wargaming as a Learning Experience and Key Assumptions Check*, https://madsciblog.tradoc.army.mil/281-would-you-like-to-play-a-game-wargaming-as-a-learning-experience-and-key-assumptions-check/, retrieved on 21 May 2024.
28. *The NATO Alternative Analysis Handbook*, 2nd edition. (2017) Norfolk: NATO Allied Command Transformation.

ADAPTATION OF THE MILITARY ORGANISATION – AN ESSENTIAL CONDITION FOR OBTAINING SUCCESS ON THE BATTLEFIELD –

Lieutenant Colonel Senior Instructor Claudiu Valer NISTORESCU, PhD

Command and Staff Faculty,
"Carol I" National Defence University, Bucharest
10.55535/RMT.2024.3.10

One of the most significant challenges that military organisations must overcome is the ability to adapt during a conflict, regardless of its scale and intensity. This complex phenomenon begins and unfolds continuously from the period of peacetime, intensifying in wartime in order to recalibrate the possibilities of the military entity to the new requirements of the battlefield. It is frequently misunderstood and inadequately researched, which has resulted in a series of adverse consequences for the actions of the armed forces. Furthermore, the absence or inadequacy of adaptation has, on numerous occasions, led to the failure of armed forces in combat, ultimately resulting in the loss of the war. In this context, the objective of this approach is to ascertain the components of the military organisation's adaptation process, its levels of achievement and the factors that contribute to its success or failure. In order to achieve the proposed objectives, a comprehensive documentary analysis has been conducted, enabling the identification of the underlying foundations of the adaptation process. Taking into account the latter, the analysis of various military conflicts from the perspective of the adaptation process has facilitated the achievement of the research results. These results, in the author's opinion, represent a topic of interest for military leadership, particularly given that the topic addressed is not sufficiently treated by the existing literature.

Keywords: military organisation; adaptation; doctrine; leadership; adaptation's key factors;

INTRODUCTION

The process of adaptation is an inherent and constant aspect of the existence of organisations. It encompasses more than simply modifying the organisation in order to enable it to respond effectively to new challenges in the environment in which it operates. The adaptation of the military organisation is a special phenomenon, and one that is much more difficult to achieve than that experienced by civilian organisations. In contrast to other organisations, military organisations in peacetime must prepare for war. War, a distinct phenomenon of humanity, may materialise at any time in the future, although there is no certainty as to when it will begin. Furthermore, war may be waged against an opponent that the military organisation is not in a position to identify or properly assess. The context of armed confrontation is characterized by a backdrop of violence, friction, chaos, uncertainty and fear, which cannot be replicated in peacetime. The use of a multitude of technologies by opponents in a concerted manner is a key factor in the conduct of armed conflict. These technologies are continually being adapted and developed in order to gain an advantage on the battlefield. It is possible that estimates of the social and political conditions in which war is fought may be inaccurate, as the impact of these conditions has implications for the development of the military organization. Furthermore, in an armed confrontation, the costs of the failure of the military organisation are much more profound than those of the failure of civilian organisations. These distinctions give rise to the specificity of the military organisation, including its adaptation process. At the same time, the aforementioned factors highlight the difficulty of measuring the results of peacetime activities in order to prepare the military organisation for war.

The adaptation of the military organisation is a special phenomenon, and one that is much more difficult to achieve than that experienced by civilian organisations. In contrast to other organisations, military organisations in peacetime must prepare for war. War, a distinct phenomenon of humanity, may materialise at any time in the future, although there is no certainty as to when it will begin.

The period following the Second World War saw a rapid acceleration in technological development, which brought about a correspondingly accelerated pace of change in military organisations.

In order to describe this phenomenon, the Soviet Union introduced the concept of *Military Technical Revolution*, while the Western states, particularly the USA, adopted the term *Revolution in Military Affairs*, the latter remaining enshrined to this day. (Sloan, 2008, p. 8). Although the necessity and reality of continuous change were apparent, the theorisation and description of this phenomenon were relatively reserved. In 1984, Barry Posen's paper *The Sources of Military Doctrine* initiated a new trend in the scientific community to research the phenomenon of military organisational adaptation. In 1990, Elliot A. Cohen and John Gooch published *Military Misfortune – The Anatomy of Failure in War*, a comprehensive work analysing the causes of failure in war. One of the causes identified was ineffective adaptation. The work was reissued in 2006, offering a new approach also from the perspective of contemporary warfare. In a 2009 publication, named *Military Adaptation in War*, Williamson Murray identifies a number of factors that contribute to the success or failure of adaptation. David Barno and Nora Bensahel, in *Adaptation under Fire* (2020), identify the key components of military adaptation and describe how it can be achieved at all levels of military operations. They focus in particular on unconventional and asymmetric conflicts. The ongoing Russian-Ukrainian conflict has ensured continued interest among the scientific community in the topic of military adaptation. In his latest publication, *The War for Ukraine: Strategy and Adaptation under Fire*, Australian General Michael Ryan offers a detailed analysis of this phenomenon, particularly in the context of the demands of today's battlefield.

David Barno and Nora Bensahel, in Adaptation under Fire, identify the key components of military adaptation and describe how it can be achieved at all levels of military operations. They focus in particular on unconventional and asymmetric conflicts.

In conceptual terms, scholastics define adaptation as the process that is characteristic of the period of conflict. The adjustments made by the military organisation during peacetime are often described by the concept of innovation (Murray, 2009, pp. 1-2). It is not uncommon for military organisations, despite their efforts to innovate and adapt effectively, to fail to do so. Failure *"to learn"*, for example, can lead to failure to adapt, and failure *"to anticipate"* can also lead to failure to adapt (Cohen, 2006, p. 63). It is similarly evident that in numerous instances, adaptation has been successfully achieved through innovation in peacetime and effective adjustments during conflict (Finkel, 2011). Concurrently, it is imperative that adaptation should be achieved in a unified and comprehensive manner at all levels of operations, encompassing both institutional and tactical aspects (Ryan, 2024). In this context, it is unclear why military adaptation is so challenging, particularly given that military entities do not always succeed in achieving it in a satisfactory manner. To address this question, we have formulated several subsequent questions, which are intended to direct the research effort:

- *What are the constituent elements of military adaptation?*
- *What are the factors that contribute to the successful adaptation of the military to new circumstances?*
- *What are the factors that contribute to the failure of military adaptation?*

In order to address these questions, an interpretative analysis of the military phenomenon was conducted from the perspective of adaptation during the course of conflicts. Both conventional and non-conventional armed conflicts have been considered, with a particular focus on modern warfare, starting with its 2nd generation. In order to achieve our stated objectives, we have undertaken an investigation into the processes of adaptation at tactical and institutional levels. In both cases, we found it necessary to determine the extent of the propagation of the phenomenon (top-down and bottom-up) in order to identify the factors influencing adaptation. The results obtained serve as theoretical benchmarks that can inform the implementation of innovation and transformation in peacetime and adaptation in the context of national armed forces engagement in conflict.

A comprehensive study on the lethality of weapon systems by Stephen Biddle reveals that, from 1900 to the present day, the lethality of major weapon systems has increased more than tenfold, yet the number of resulting casualties has decreased steadily. It is a consequence of the innovative and adaptive approach adopted by the armed forces.

A HISTORICAL PERSPECTIVE OF MILITARY ADAPTATION'S EVOLUTION

A comprehensive study on the lethality of weapon systems by Stephen Biddle reveals that, from 1900 to the present day, the lethality of major weapon systems has increased more than tenfold, yet the number of resulting casualties has decreased steadily (Biddle, 2004, p. 23). It is a consequence of the innovative and adaptive approach

adopted by the armed forces. Prior to the First World War, the pace of innovation and adaptation was relatively slow. The *"lines and columns"* tactics employed in the early days of modern warfare limited the scope for doctrinal transformation. The advent of new technologies has brought advantages at the tactical level, yet they have not been sufficient to alter the fundamental rules of the game and to influence the outcome of battles decisively. The conservatism inherent in military organisations has led to a doctrinaire approach cantered on the Clausewitzean idea of the *"decisive battle"*, which is justifiable given the performance of weapon systems.

The development of sea and rail transportation provided the military with unprecedented strategic mobility. It facilitated the concentration of vast numbers of troops by all the belligerents in the First World War.

By the end of the 19th century, the advent of the machine gun represented a significant advancement in military technology, marking a pivotal shift in warfare. The principle of recoil energy recovery enabled the weapon to fire at a much faster rate than previous firearms, making it a pivotal weapon in the modern era. It resulted in the abandonment of tactics and combat techniques based on the principle of lines and columns, and forces were compelled to disperse on the battlefield. It is evident that there has been an adaptation of battle tactics and procedures, yet the approach to operations has remained unchanged. The development of sea and rail transportation provided the military with unprecedented strategic mobility. It facilitated the concentration of vast numbers of troops by all the belligerents in the First World War. However, the lack of tactical mobility resulted in an operational stalemate, which eventually led to the emergence of what became known as *"trench warfare".* The combatants sought solutions to overcome the stalemate of positional warfare. The use of chemical weapons was highly unpredictable and could easily be countered by wearing protective masks. The development of the airplane and tank was in its infancy, with their use on the battlefield being sporadic and with little significant impact. Both combatants ended up increasing the firepower of their artillery, making defence the favoured form of combat. Enemy positions were hard to take, and once taken, they were even harder to hold.

In the interwar period, technological innovations gave rise to a series of military innovations. The German armed forces established a doctrine based on the principle of *combined arms*, which informed the organisation of armoured divisions and the tactics they employed. The development of the tank and the air force paved the way for the integration of air-ground operations. The means of radio communications facilitated the implementation and exercise of *Auftragstaktik* – the command philosophy of the German armed forces. The Germans integrated armoured action with dive-bomber support, all coordinated by means of radio communications, demonstrating a capacity to adapt at the tactical level, which was doctrinally and operationally surprising to the French and later the Soviet armed forces. However, although the Germans demonstrated a high capacity to adapt at the tactical level, the institutional adaptation at the strategic level was dysfunctional, and Germany was ultimately defeated. Mission command, a foundation of German military thinking, was exercised only at the tactical level of operations.

The French primarily utilized tanks in support of infantry operations or for limited pursuit actions. The speed of movement of the tactical structure was contingent upon the speed of the infantry units, in contrast to the German approach, where the tank set the pace for the entire joint structure.

France, despite possessing comparable technological capabilities to Germany, encountered difficulties in integrating these capabilities effectively at the force structure level. It resulted in a lack of innovation and, consequently, a failure to adapt doctrinal approaches during the 1940 campaign. The French primarily utilized tanks in support of infantry operations or for limited pursuit actions. The speed of movement of the tactical structure was contingent upon the speed of the infantry units, in contrast to the German approach, where the tank set the pace for the entire joint structure. Aviation missions were conducted independently, with a primary focus on strategic operations. There was a notable absence of integration between air and ground operations. Radios were utilized as an alternative to other forms of communication and were at the level of combat sub-units. Furthermore, the hesitation of high-ranking commanders, including General Gamelin, to utilize and integrate radio communications at the tactical level contributed to the cumbersome conduct of operations. (Beevor, 2015, p. 98).

In the initial phase of *Operation Barbarossa*, the Soviet armed forces disregarded the lessons learned from the Napoleonic campaigns. Instead of implementing a *"manoeuvre defence"*, which would have led to the expansion of the German armed forces lines

of communication thus absorbing the shock of the German offensive, they concentrated the efforts on a defence in position. (Bartles, 2022). The inflexible command system, in conjunction with the political factor's interference in planning and conducting military operations, impeded the Russians' adaptation process, resulting in significant human and territorial losses. Despite the Russians' quantitative advantage in terms of human resources and combat technique, the Germans, through extensive envelopment manoeuvres, managed to encircle and destroy approximately two million soldiers in less than six weeks, a rate of attrition that was tenfold greater than their own losses. (Roberts, 2020, pp. 317-323). The *Battle of Stalingrad* can be considered the starting point of the Soviet armed forces adaptation process. The reduction of excessive command control and the confidence instilled in military commanders created the necessary conditions for tactical adaptation. The adaptation of tactical operations was also supported by an adaptation at the level of the entire armed forces, through the forced but effective mobilization of the population and the intensification of the war industry. *Table 1* provides a schematic illustration of the manner in which the three belligerents were able to adapt their strategies in relation to the doctrine that had been implemented prior to the commencement of hostilities.

The Battle of Stalingrad can be considered the starting point of the Soviet armed forces adaptation process. The reduction of excessive command control and the confidence instilled in military commanders created the necessary conditions for tactical adaptation.

Table 1: The adaptation of the German, French and Soviet armed forces in the context of the Second World War (author's design)

	Doctrine	Tactical adaptation	Institutional adaptation
German Armed Forces	correct	yes	no
French Armed Forces	wrong	no	no
Soviet Armed Forces	wrong	yes	yes

In 1973, the Egyptian armed forces sought to avenge their 1967 defeat in the *Six-Day War* by employing a technological and doctrinal surprise attack on the Israeli armed forces. The *Yom Kippur War*, as it came to be known, found the Israeli armed forces unprepared and beholden to an outdated doctrine. The fundamental principle of the Israeli doctrine was the use of tank structures to penetrate the depth of the enemy's defence, while holding air superiority and benefiting from constant air force support. The failure to anticipate the need to change the doctrinal approach, in light of the development of new weapon systems such as guided anti-tank missiles and ground-to-air anti-aircraft missile systems, contributed to the failure of the Israeli armed forces in the initial phase of the operation. Finally, the tendency of Israeli military leaders to underestimate the Egyptian armed forces and to approach the military phenomenon exclusively from the perspective of their own experience of previous wars delayed the reconsideration of the doctrine. Nevertheless, the Israeli armed forces, which had a high degree of flexibility in their leadership, were able to adapt to the unexpected and ultimately emerge victorious. (Kober, 2011, p. 177). In contrast, the Egyptian armed forces, which benefited from an innovative doctrine, failed to adapt during the conflict, despite the initial success. The main cause for the mentioned failure was the significant interference of the politico-military leadership in setting tactical-operational objectives and conducting operations. The rigid command system did not allow the exploitation of strategic surprise, superior doctrine and significant technological advantage. The adaptation of the two armies in the conflict, which commenced from disparate doctrinal foundations, is illustrated schematically in *table 2*.

The Israeli armed forces, which had a high degree of flexibility in their leadership, were able to adapt to the unexpected and ultimately emerge victorious. In contrast, the Egyptian armed forces, which benefited from an innovative doctrine, failed to adapt during the conflict, despite the initial success.

Table 2: The adaptation of the armed forces of Israel and Egypt during the Yom Kippur War (author's design)

	Doctrine	Tactical adaptation	Institutional adaptation
Israeli Armed Forces	wrong	yes	yes
Egyptian Armed Forces	correct	no	no

Another conflict that merits our attention is the *Vietnam War*. The superior firepower of the US military proved insufficient to defeat the North Vietnamese forces and Vietcong guerrillas, who were able

to quickly overrun American-held territory. The lack of adequate doctrine required American forces to adapt, often at significant cost in terms of casualties among the soldiers. From a technological standpoint, the tactical adaptation was relatively slow. The malfunctions identified by the soldiers were often downplayed, with the M16 assault rifles being a notable example. These malfunctions significantly affected the soldiers' morale (O'Connell, 2020). Perhaps the most significant reason for inadequate adaptation was the failure of senior leaders to understand the type of war they were fighting and the enemy they were dealing with. General Westmoreland, Commander of the US forces in Vietnam for four years, repeatedly referred to his combat experience from the Second World War and the Korean War. It resulted in a lack of adaptability to the specifics of the battlefield (Bensahel, 2020, p. 98).

General Westmoreland, Commander of the US forces in Vietnam for four years, repeatedly referred to his combat experience from the Second World War and the Korean War. It resulted in a lack of adaptability to the specifics of the battlefield.

The US Armed Forces, through the Department of Training and Doctrine/TRADOC, developed the *AirLand Battle* doctrine in the context of the Yom Kippur War. The doctrine was designed to ensure victory in a potential confrontation with the Soviet Union, based on the technological outrunning of the enemy while integrating air-to-ground operations and expanding the battlefield in space and time. The doctrine was to be tested in the 1991 *Gulf War*, ensuring coalition forces a resounding success. The same doctrine gave US forces a quick victory in *Iraq* in 2003, but the inability to anticipate the potential of a large-scale insurgency created serious problems in adapting doctrine and technology. The lack of a doctrine to counter insurgency was also due to the US military's unwillingness to retain expertise in this area after its *Vietnam War* experience.

Since the conclusion of the Cold War, Western militaries have gradually developed doctrines to respond effectively to unconventional and asymmetric conflicts, such as those in Iraq and Afghanistan. Technologies have also been adapted, and superiority in this area has given NATO forces dominance in all areas of operations. This new reality, inherently, has resulted in the blurring and loss of some of the knowledge of large-scale armed combat operations, and the capabilities for this form of armed confrontation have also been greatly reduced. Perhaps the most damaging consequence of the aforementioned developments has been the shift in perspective among military

leaders regarding conventional warfare. In the current context, it is of paramount importance to facilitate a mental recalibration among these leaders, as well as to reconsider military doctrines in an environment marked by unprecedented technological developments.

MILITARY ADAPTATION COMPONENTS

A historical perspective on military adaptation reveals the inherent challenges of such a process and its role in achieving success on the battlefield. Factors inherent in the nature of warfare, such as friction, chance, uncertainty, chaos and fear, present obstacles to adaptation. Conversely, the following factors, which define the nature of war, directly and variably influence adaptation: doctrine, technology and leadership. Research findings highlight the role of the latter in a highly hostile environment. In this context, it is pertinent to cite the views of Nora Bensahel and David Barno, *"Rigid doctrine, inflexible technology, and dogmatic leaders are a recipe for disaster, given the uncertainty, chaos, and surprises that characterize every war"* (Bensahel, 2020, p. 22). In light of the empirical results presented, the following components of adaptation have been identified: *doctrinal, technological, leadership components*.

"Rigid doctrine, inflexible technology, and dogmatic leaders are a recipe for disaster, given the uncertainty, chaos, and surprises that characterize every war".

❖ *The role of the doctrinal component*

The term *doctrine* has its roots in Latin and is used to describe both an *accumulation of teachings* and a *set of instructions*. The content of doctrine emphasises both its descriptive and educative aspects, as well as its prescriptive nature. The concept of *military doctrine* is concerned with how the military organisation generates, plans, organises, trains and deploys its available resources in order to achieve its military objectives, within the context of the national security policy, including the *"grand strategy"* of the state (Posen, 1986, p. 13). The formulation of doctrine for a given period of time is a complex and continuous process, requiring adjustments as a result of reassessment of the security environment, the new characteristics of the operating environment, the potential threat and the capabilities available. In this regard, J.F.C. Fuller, more than a century ago, stated that *"formal doctrine develops in peacetime and continues to evolve*

in times of conflict". (UK Ministry of Defence, Development, Concepts and Doctrine Centre, 2011, p. 2.2).

In the context of preparing the military organisation for war, the doctrine must regularise its activity and provide a series of predictable outcomes regarding the evolution of the military phenomenon:

- It should be sufficiently flexible to adapt to the ever-changing circumstances of the battlefield.;
- the regulatory function of the organisation enables it to make a relevant assessment of the battlefield and identify the need for change;
- the predictive function enables the identification of doctrinal solutions and their integration at all levels of operations;
- following the dissemination of new doctrinal ideas, it is necessary to conduct a rapid evaluation in order to obtain feedback on their effectiveness.

It is essential for the military organisation to be aware of the possibility of a need for change and to mentally accept it, facilitating the transformation of doctrine as needed. Only in this way will adaptation be timely and effective, contributing to success.

In light of these milestones, it becomes evident that there is a necessity for military doctrine to be more descriptive than prescriptive. It would allow commanders to act on principles rather than be constrained by detailed regulations. It is also important to consider that while a doctrine may be effective at the outset of a military confrontation, this aspect may not be sufficient. Furthermore, the possibility of adapting an inappropriate doctrine may outweigh the benefits of a precise but inflexible doctrine. In this context, it is essential for the military organisation to be aware of the possibility of a need for change and to mentally accept it, facilitating the transformation of doctrine as needed. Only in this way will adaptation be timely and effective, contributing to success.

❖ *The role of the technological component*

New technologies have consistently influenced the character of warfare, as military forces strive to incorporate them into their new weapons systems. Military conflicts have demonstrated that military victory is contingent not only on the quality of weaponry, but also on the quality of weapon-carrying platforms and the equipment that integrates them (Scipanov, Totir, 2023). Technological adaptation can yield noticeable results in the short term, helping to temporarily solve

a problem. However, effective adaptation also requires technological adaptation at the institutional level. In the initial phase of the conflicts in Iraq and Afghanistan, US military personnel worked to improve the armour of HMMWVs to increase protection against hits from portable grenade launchers and improvised explosive devices. Subsequently, the US Army developed and integrated MRAP and MATV vehicles into its forces, designed to withstand these threats. Given the above, I would like to draw attention to some concepts that are relevant to technological adaptation, at both tactical and institutional levels:

- it is important for low-level leaders to be aware of the potential for encountering technological issues and to be willing to address them in a creative manner;
- it is necessary to identify a mechanism that will allow the implementation of adjustments as close as possible to the operational area;
- the rapid dissemination of temporary technological solutions for deployment by all units is a crucial aspect of this process;
- the objective is to maintain communication between the organisation's decision-making bodies and the leaders of the tactical level structures in order to identify any technological malfunctions or shortcomings;
- the necessity to overcome bureaucratic obstacles in order to implement change in a timely manner.

In the initial phase of the conflicts in Iraq and Afghanistan, US military personnel worked to improve the armour of HMMWVs to increase protection against hits from portable grenade launchers and improvised explosive devices. Subsequently, the US Army developed and integrated MRAP and MATV vehicles into its forces, designed to withstand these threats.

Nevertheless, despite the organisation's endeavours to adopt technological advances, this process may prove unsuccessful, particularly due to shortcomings in the management of other adaptation components. Consequently, it is imperative to achieve a unified approach to the various components of military adaptation.

❖ *The role of the leadership component*

The adaptation of leadership in wartime is a challenging endeavour, considering that *"some systems of command make adaptation to unexpected or unforeseen circumstances relatively easy, while others make it virtually impossible"* (Cohen, 2006, p. 451). It is leaders who initiate the adaptation process, both at both tactical and institutional levels. It is through them that the components of military adaptation

are linked at all operational levels. In order to meet these demands, leaders must be adaptive. Thus, they must:

- rapidly assess the situation on the battlefield and identify the necessity for change;
- cease utilising procedures that are no longer aligned with the demands of the battlefield while identifying and implementing suitable alternatives;
- the utilisation of effective reporting mechanisms is imperative to ensure that any issues pertaining to the efficacy of tactics and procedures, or the suitability of weapons and combat techniques, are brought to the attention of the relevant authorities in a timely and transparent manner;
- identify promising concepts, to allocate the necessary resources to their development, and to coordinate the efforts required to implement them.

It is a fundamental objective of all military organisations, whether in peacetime or wartime, to identify the optimal formula (encompassing conceptual, educational, organisational, technological and command-related factors) to guarantee their success on the battlefield.

THE FACTORS THAT CONTRIBUTE TO THE SUCCESS OR FAILURE OF MILITARY ADAPTATION

It is a fundamental objective of all military organisations, whether in peacetime or wartime, to identify the optimal formula (encompassing conceptual, educational, organisational, technological and command-related factors) to guarantee their success on the battlefield. Adaptation is a universal experience among combatant entities, irrespective of the outcome of a specific battle or the overall conflict (Ryan, 2024). In this context, it is not possible to precisely define success or failure in adaptation. However, we have identified a number of factors that contribute to or, on the contrary, hinder success on the battlefield. Factors facilitating success in military adaptation include:

- the existence of a comprehensive and coherent understanding of the nature and scope of military adaptation;
- the objective is to achieve military innovation, taking into account the lessons learned from conflicts and existing trends in the changing character of warfare;
- the identification of potential triggers that can become decision points for initiating change;

- the identification of risks associated with the initiation and implementation of the adaptation process;
- the assessment of adaptation processes entails the implementation of performance and efficiency indicators;
- the establishment of a functional framework for the rapid correction of weaknesses and malfunctions identified by the evaluation is a crucial step in the process;
- the identification and assessment of potential threats, in order to direct innovation and adaptation to neutralize or mitigate them in the event of military conflict;
- the training of leaders to accept failure, to be aware of the need to adapt and to demonstrate initiative in initiating the process.
- In a similar vein, a number of factors have been identified which limit the adaptability of the military organisation in times of conflict:
- the excessive bureaucratisation of military organisations through the implementation of a series of standard operating procedures, functional rules and regulations is intended to reduce uncertainty. However, change inherently generates uncertainty, and thus bureaucracy is an impediment to change;
- the continued implementation of ineffective military equipment programmes by politico-military decision-makers, despite the evaluation of the adaptation process, represents a significant obstacle to the advancement of military capabilities;
- a lack of investment in research and development (R&D) programmes;
- the failure to take into account indicators and reports from the battlefield that highlight ineffective tactics, techniques and procedures/TTPs or ineffective weapons systems;
- the failure to apply the lessons learned during peacetime constitutes a missed opportunity for learning. Furthermore, the neglect of lessons identified during conflict impedes the pace of adaptation, at both tactical and institutional levels;
- the implementation of a unidirectional, top-down institutional adaptation, without consideration of feedback from the beneficiary;

The failure to apply the lessons learned during peacetime constitutes a missed opportunity for learning. Furthermore, the neglect of lessons identified during conflict impedes the pace of adaptation, at both tactical and institutional levels.

- the organisation's rigidity in accepting new doctrinal ideas and integrating new technologies;
- the continued use of outdated technologies and equipment in the context of armed conflict can have significant implications for the operational effectiveness of military forces. These technologies and equipment may become vulnerable to disruption or destruction, leading to a chain of malfunctions that can rapidly collapse the operational capabilities of the armed forces engaged in operations;
- a lack of effective implementation and exercise of mission command.

The permanent contradiction between maintaining a high degree of control specific to a disciplined organisation and the need to adapt quickly is one of the dilemmas of politico-military decision-makers. Bureaucracy and a strict command system can slow down or even block adaptation initiatives.

CONCLUSIONS

The results of this analysis provide an answer to the question of *why military adaptation is so difficult*. One of the main reasons that hinder effective adaptation is the organisation's resistance to change. The permanent contradiction between maintaining a high degree of control specific to a disciplined organisation and the need to adapt quickly is one of the dilemmas of politico-military decision-makers. Bureaucracy and a strict command system can slow down or even block adaptation initiatives. Furthermore, a philosophy of detailed command will not provide subordinate commanders with the requisite *"power"* to act in accordance with the commander's intent to capitalise on opportunities on the battlefield. The prospect of having to relinquish some peacetime innovations that have entailed significant material costs also makes adaptation challenging. Additionally, the reluctance of high-level leadership to recognise and acknowledge the existence of dysfunctions in peacetime force preparation, the erroneous anticipation of the nature of war, or the lack of proper implementation of new doctrinal concepts also create the preconditions for slow adaptation. Finally, the inability of the organisation to integrate new technologies or to modify or adapt its doctrine in order to exploit those technologies contributes to a reduction in the effectiveness of adaptation.

In light of the empirical evidence, it is imperative to adopt an adaptive approach to armed combat and warfare in general.

The success of adaptation is contingent upon the success of peacetime innovation in key areas such as military doctrine, the forces organisation and training, and their equipment with new technologies and weapon systems. The more effective this innovation is, the quicker and less costly the adaptation will be. It necessitates a continuous and frank evaluation of the process, with the establishment of performance and efficiency indicators. Concurrently, in order to guarantee the successful adaptation of the military organisation in times of conflict, it is essential to direct particular attention to the past, with the analysis and lessons learned from previous conflicts also being carried out from the perspective of adaptation. The failure to acknowledge historical precedents may result in the perpetuation of past errors. However, it is crucial to recognise the potential pitfalls of relying solely on past experiences and knowledge, particularly in the context of evolving conflict dynamics. In this regard, it is essential for leaders to demonstrate adaptability, while institutions must cultivate an environment conducive to such flexibility. The implementation and exercise of *mission command*, the command philosophy adopted by Western armed forces, including the Romanian Armed Forces, appear to be a solution that facilitates the creation of a framework that enables both innovation and adaptation.

The success of adaptation is contingent upon the success of peacetime innovation in key areas such as military doctrine, the forces organisation and training, and their equipment with new technologies and weapon systems.

The Russian-Ukrainian conflict provides a contemporary illustration of the process of adaptation of the military organisation during an unconventional conflict between two opponents with relatively equal capabilities. Both combatant states make substantial efforts to adapt, which represents the essence of the strategy used to win the war. Adaptation takes place not only at the tactical level of operations but also at the institutional level. Tactics and combat procedures are adjusted to ensure a position of advantage while increasing the chances of survival on the battlefield. The organisation of tactical structures is in a constant state of flux, striving to meet the demands of operations in urban environments or the necessity to disperse forces, while also integrating new technologies and weapon systems. Concurrently, both countries are attempting to streamline their recruitment activities and enhance the training of their forces, while simultaneously reinvigorating

the war industry. During this process of adaptation, decision-makers, both political and military, consider the needs on the battlefield, the economic possibilities of the state, the readiness of allies, the determination of the population to support the war effort and the time prospects of the war. It is challenging to forecast the outcome of this conflict, but it is evident that the adaptation of the military organisation will be a decisive factor. The precise doctrinal fine-tuning, effective integration of new technologies and flexible leadership at all levels of operations, and at a faster pace than the enemy will most likely set the stage for success on the battlefield.

During this process of adaptation, decision-makers, both political and military, consider the needs on the battlefield, the economic possibilities of the state, the readiness of allies, the determination of the population to support the war effort and the time prospects of the war.

BIBLIOGRAPHY:

1. Bartles, L.W. (2022, winter). *The Russian Army and Maneuver Defense*. In *Armor*.
2. Beevor, A. (2015). *Al Doilea Război Mondial.* București: Rao Class.
3. Bensahel, D.B. (2020). *Adaptation under Fire – How Militaries Change in Wartime.* Oxford: Oxford University Press.
4. Biddle, S. (2004). *Military Power, Explaining Victory and Defeat in Modern Battle.* New Jersey: Princeton University Press.
5. Cohen, E.A., Gooch, J. (2006). *Military Misfortunes.* New York, London, Toronto, Sydney: Free Press.
6. Finkel, M. (2011). *On Flexibility-Recovery from Technological and Doctrinal Surprise on the Battlefield.* California, USA: Stanford Security Studies, Stanford University Press.
7. Kober, A. (2011). *The Evolution of Operational Art from Napoleon to The Present.* (M. v. John Andreas Olsen, Ed.) Oxford: Oxford University Press.
8. Murray, W. (2009). *Military Adaptation in War.* Alexandria, Virginia, USA: Institute for Defense Analyses.
9. O'Connell, J. (2020, April). *The M16 in Vietnam: A History of the Weapon's Effectiveness in the Vietnam War and the Necessity of its Creation*. In *Philologia*. DOI:10.21061/ph.228
10. Posen, B.R. (1986). *The Sources of Military Doctrine.* Ithaca and London: Cornell University Press.
11. Roberts, A. (2020). *Furtuna Războiului*. București: Editura Litera.
12. Ryan, M. (6 May 2024). *Ukraine and Military Adaptation*. In *Futura Doctrina*, https://mickryan.substack.com/p/ukraine-and-military-adaptation, retrieved on 12 May 2024.

13. Scipanov, L.V., Totir, V.C. (2023). *The Need to Adapt Naval Tactics to Technological Evolution. Drones and Drone-Carrying Platforms*. In *Romanian Military Thinking*, Defence Staff, no. 3/2023, pp. 36-55.
14. Sloan, E. (2008). *Military Transformation and Modern Warfare: A Reference Handbook.* UK: Praeger Security International.
15. UK Ministry of Defence. Development, Concepts and Doctrine Centre. (2011). *Army Doctrine Primer.* Army Doctrine Publication.

ROMANIAN MILITARY THINKING

ROMANIAN
MILITARY
THINKING

EMERGING TECHNOLOGIES IN MILITARY CONFLICTS – ETHICAL AND LEGAL IMPLICATIONS –

Cristina Elena VASILACHE
"Henri Coandă" Air Force Academy, Brașov
Loreta Daniela MAZILU
"Transylvania" University, Brașov
10.55535/RMT.2024.3.11

Technological advancements are radically transforming the conduct of military conflicts. While these innovations offer significant operational advantages, they also raise major ethical and legal challenges. This study examines the impact of emerging technologies on the legitimacy of military actions and the decision-making process, emphasizing the necessity for robust legal and ethical frameworks to ensure compliance with international norms. The military system must align with technological requirements to meet training needs and the dynamics of the operational environment. The integration of Extended Reality (xR) into the decision-making process is essential for a robust and future-ready defence system. The study calls for a nuanced approach to integrating these technologies, balancing technological advantages with ethical obligations.

Keywords: legitimacy of military actions; decision-making processes; autonomous systems; ethical concerns; extended reality; artificial intelligence;

INTRODUCTION

Technological advances are converging towards the intensification of military conflicts through the escalation of arming with technologies. These aspects can generate uncertainty regarding military actions and can complicate the identification of responsibility for potential errors or war crimes. The use of precision weapons and drones, for example, can make military decision-makers perceive war as an easy solution without repercussions, as they can avoid collateral damage and the loss of their own human lives. This technological capability may foster emotional detachment, making the justification of military actions easier and reducing the perceived level of moral responsibility in decision-making.

The following analysis examines the use of modern technologies in warfare through the lens of military implications and adherence to international laws. The significant aspects of modern technologies encompass a wide range of fields, including artificial intelligence (AI), autonomous systems weapons, robotics, cyber warfare, precision-guided munitions, and advanced communication systems. These technological advancements bring significant ethical challenges, particularly regarding the determination of responsibility for actions taken by AI and autonomous systems. In this context, questions arise, such as: *Who is responsible for the actions taken by autonomous weapon systems? What is the impact on human rights and the necessity of protecting civilians? How can we control these technological advancements, especially their proliferation among non-state actors?*

The significant aspects of modern technologies encompass a wide range of fields, including artificial intelligence, autonomous systems weapons, robotics, cyber warfare, precision-guided munitions, and advanced communication systems. These technological advancements bring significant ethical challenges, particularly regarding the determination of responsibility for actions taken by AI and autonomous systems.

The legitimacy of military actions is fundamentally built, maintained, and sustained through adherence to international legal standards for the use of force, respect for the rule of law, protection of civilians and civilian infrastructure. Legitimacy in military actions encompasses legal, moral, ethical, political, and social dimensions. International debates regarding the legal framework for new technologies, especially autonomous weapon systems, are current and intensely discussed,

particularly by the International Committee of the Red Cross (ICRC). The persistent issue is *how to apply the set of rules/principles in AI algorithms.* Moreover, the sanctions that can be imposed for non-compliance with these rules, compared to the advantages of using these technologies, are disproportionate, making it even more difficult to control them.

In this brief analysis, based on principles identified from international laws and frameworks developed by the ICRC, we discuss a *"Model of integrating ethical war principles into AI algorithms for autonomous weapon systems"*. This model identifies the principle, the rule, and the way to implement it into the algorithm. Moreover, it can be adapted to new challenges identified through international law and must be used by all AI developers. Besides the autonomous weapons and the discussions surrounding their use on the battlefield, the last part of the paper argues for integrating Extended Reality in the military decision-making process as a component of mission preparation.

In the context of unstable international security, any delay in updating procedures and adopting emerging technologies can create significant disparities between different armed forces, potentially having major implications for global security.

This study highlights the critical need for the military system, particularly the Romanian military, to adapt to the rapid advancements in technology, considering both their positive and negative implications. In the context of unstable international security, any delay in updating procedures and adopting emerging technologies can create significant disparities between different armed forces, potentially having major implications for global security.

CLARIFYING TERMINOLOGY IN THE CONTEXT OF EMERGING TECHNOLOGIES

In the context of current discussions about emerging technologies, it is essential to clarify the terminology to avoid confusion between *Artificial Intelligence (AI), Augmented Intelligence (IA), Extended Reality (xR)*, and *Autonomous Weapon Systems (AWS).* In the specialized literature, these terms are relatively new, creating ambiguity in their usage due to their intersection and complementarity around the concepts of algorithms and augmentation.

The abbreviation *"AI"* is widely recognized and accepted for *Artificial Intelligence*. AI refers to the technology that enables machines to perform tasks that typically require human intelligence, through the use of algorithms and information processing techniques.

Augmented Intelligence – *"IA"* refers to the use of advanced technologies to enhance and extend human capabilities. The primary goal of IA is to assist people in decision-making and performing complex tasks, rather than replacing them. Although the term is often confused with AI, augmented intelligence combines artificial intelligence with human expertise, providing support for data analysis, predictions, and recommendations. It is used in various fields, including medicine, finance, and industry, to improve productivity and accuracy.

"AWS" is a recognized term for *Autonomous Weapon Systems*, which are systems capable of selecting and engaging targets without direct human intervention. Autonomous weapon systems are specific applications that use AI to operate independently, making decisions without human input. The use of this term is common in discussions about the ethics and legality of autonomous weapons.

AI also plays a significant role in *Extended Reality (xR)*, which is an umbrella term covering all technologies that combine real and virtual elements to create interactive and immersive experiences. xR includes *Virtual Reality (VR), Augmented Reality (AR*), and *Mixed Reality (MR)*. AI enhances xR experiences by optimizing user interactions and personalizing content based on user preferences. For example, AI can adapt the virtual environment in real time to create more effective training scenarios or provide real-time assistance in industrial applications. To ensure clarity and coherence in this article, we will use the following terminological conventions:

Augmented intelligence combines artificial intelligence with human expertise, providing support for data analysis, predictions, and recommendations. It is used in various fields, including medicine, finance, and industry, to improve productivity and accuracy.

- *"AI"* for *Artificial Intelligence*;
- *"IA"* for *Augmented Intelligence*;
- *"AWS"* for *Autonomous Weapon Systems*;
- *"xR"* for *Extended Reality*, including VR, AR, and MR.

THE LEGITIMACY OF MILITARY ACTIONS IN THE CURRENT CONTEXT OF TECHNOLOGICAL EVOLUTION

Legitimacy in military actions refers to the conformity of such actions with nationally and internationally recognized norms, principles and standards. It involves both legal and ethical justification for the use of force, ensuring that the actions taken are seen as acceptable and justified by the international community and the wider

public. Legitimacy in military actions is crucial as it impacts the perceived justice and support for these actions, both domestically and internationally. Without legitimacy, military actions may face significant opposition, undermine international relations, and lead to long-term conflicts and instability. International Humanitarian Law (IHL), Just War Theory and other ethical frameworks provide moral justification for military actions, making them appear more just. Key principles like just cause, right intention, and proportionality are essential in this regard. This concept is multidimensional and encompasses legal, moral, and social perspectives.

The debate over the legitimacy of military actions in the context of current technological progress is a subject of profound significance and complexity. On the one hand, technological advances have enabled more precise and targeted military operations, reducing the potential for collateral damage and civilian casualties. On the other hand, these advances raise concerns about the disproportionate use of force and the erosion of responsibility in warfare, due to the emotional and moral distancing between those who conduct military operations and their consequences on the civilian population. Additionally, political leaders can make decisions to engage militarily without having to fully assume responsibility for these decisions. For example, in a conflict involving drones with reconnaissance and attack capabilities, political leaders might be tempted to delegate the decision-making authority for attacks to military commanders or even algorithms, thus diminishing their own responsibility. Undoubtedly, with the advent of autonomous military systems, clarity regarding lines of responsibility is diminished.

Political leaders can make decisions to engage militarily without having to fully assume responsibility for these decisions. For example, in a conflict involving drones with reconnaissance and attack capabilities, political leaders might be tempted to delegate the decision-making authority for attacks to military commanders or even algorithms, thus diminishing their own responsibility.

A recent example that raises questions about legitimacy in actions involving the use of AI algorithms and automated systems can be observed in the Israeli military operations in Gaza (Dombe, 2023). Here, the manner in which certain decisions have been made and the transfer of responsibility between political leaders and military commanders generate ambiguity. The ambiguity regarding responsibility for military actions is accentuated in situations where decisions are made by automated systems. It can lead to questions about *who* is actually responsible for the actions taken – political leaders, military commanders, or software developers. Algorithms can have errors, and decisions based on incorrect or misinterpreted data can lead to serious

consequences, including unintended civilian casualties, which would violate the principles of proportionality and distinction.

A recent investigation reveals that the Israeli military has used an AI-based system, *"Lavender"*, in operations against Gaza (Yuval, 2024). This system marks tens of thousands of Palestinians as targets with minimal human oversight, leading to significant collateral damage. *"Lavender"* software was described by officers under the protection of anonymity as having a very permissive approach regarding collateral damage, indicating that it allowed the elimination of a considerable number of civilians depending on the importance of the target. The use of AI-based systems like *"Lavender"* in Israeli military operations has led to significant civilian casualties in Gaza. According to reports, these technologies allow for more rapid targeting but have resulted in increased collateral damage. Estimates indicate around 15,000 Palestinians have been killed since 7 October 2023, with a significant portion being civilians, including many children and women.

Concerns about responsibility and ethical implications arise as decisions increasingly rely on automated systems. The use of such technology underscores the need for clear legal frameworks and limitations to prevent unintended civilian casualties and ensure responsible military conduct. The use of artificial intelligence systems such as *"Lavender"* and *"Habsora"* (known as *"Gospel"*) by the Israeli armed forces in operations in Gaza highlights the need to establish clear limits and a legal framework for these advanced technologies.

Israeli military has used an AI-based system, "Lavender", in operations against Gaza (Yuval, 2024). This system marks tens of thousands of Palestinians as targets with minimal human oversight, leading to significant collateral damage.

Recent discussions on the international stage about the legitimacy of military actions have often focused on factors such as adherence to international laws, rules of engagement and ethical considerations, which govern how armed conflicts should be conducted to protect civilians and prevent war atrocities. The use of technologies like autonomous or cyber weapons raises numerous questions about human rights, ethics, transparency, and accountability, particularly regarding how they might be integrated within international norms and regulations. Additionally, concerns about increasing power inequalities between state and non-state actors, the risk of escalating conflicts, and the possibility of losing human control over these advanced military technologies are aspects that can influence perceptions of the legitimacy of military actions.

Legal tools, such as the Geneva Conventions and the Rome Statute of the International Criminal Court, hold individuals and states accountable for war crimes, including the deliberate targeting of civilians or the disproportionate use of force. The principles of distinction and proportionality in international humanitarian law are well-founded, based on various articles from Additional Protocol I (AP I) to the Geneva Conventions. These principles aim to limit the impact of war on civilians and ensure that military actions are carried out in a way that respects human rights and international law. Thus, the principle of distinction is clarified within Additional Protocol I, obliging parties to the conflict to distinguish between combatants and civilians and to direct their actions only at military objectives. This principle aims to protect the civilian population and civilian objects from the effects of hostilities. The principle of proportionality, on the other hand, is detailed in Article 51(5)(b) of AP I, which prohibits *"Attacks which are expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination of these losses and damages, that would be excessive in relation to the concrete and direct military advantage anticipated"*. Moreover, Article 57 of AP I emphasizes the need to take all feasible precautions in the choice of means and methods of attack to minimize civilian casualties and damage to civilian objects (ICRC, 1977).

Legal tools, such as the Geneva Conventions and the Rome Statute of the International Criminal Court, hold individuals and states accountable for war crimes, including the deliberate targeting of civilians or the disproportionate use of force.

From a legal perspective, there is a solid basis for applying these essential principles and limiting the effects of armed conflicts on the civilian population by ensuring that military actions are conducted with minimal collateral damage. It means that any use of autonomous weapons and AI algorithms in armed conflicts must adhere to these principles, ensuring that appropriate measures for distinction and proportionality are implemented. However, there is a growing consensus that existing international legislation is insufficient to manage the challenges posed by emerging technologies like AI in military operations. It requires the development of new norms and regulations that align with technological innovations.

It is essential that both states and non-state actors adhere to these legal norms to reduce the human impact of conflicts and promote justice and equity during wars. However, in practice, there are

often difficulties in holding responsible individuals accountable due to the dilution of responsibility through the use of AI algorithms. Therefore, the erosion of responsibility in warfare in the context of technological progress could pose a threat to ethics and justice in armed conflicts, and research and debates on this topic are essential to maintain moral and legal standards in the military field. Clear and adequate regulation of the use of these technologies is crucial to avoid abuses and negative consequences on international security and the civilian population. To maintain ethics and responsibility, many experts suggest that critical decisions, especially those involving human targets, should remain under the strict supervision and control of human operators (United Nations, 2021).

The future of international security will likely be influenced by a combination of traditional and emerging threats, geopolitical shifts, technological advances and global challenges. Cybersecurity, emerging technologies, climate change, geopolitical competition, non-traditional security threats and multilateralism are key factors that will shape the international security landscape in the coming years. Addressing these challenges requires a coordinated global approach and collaboration between governments, international organizations, researchers and civil society.

Cybersecurity, emerging technologies, climate change, geopolitical competition, non-traditional security threats and multilateralism are key factors that will shape the international security landscape in the coming years.

ADDRESSING ETHICAL AND LEGAL CHALLENGES OF AUTONOMOUS WEAPON SYSTEMS: INTERNATIONAL EFFORTS AND FRAMEWORKS

Numerous international studies, frameworks, and initiatives aim to tackle the ethical and legal challenges posed by autonomous weapon systems (AWS) and ensure their compliance with international humanitarian law (IHL) and ethical standards. For example, the International Committee of the Red Cross (ICRC) has published several reports and papers on the implications of AWS, emphasizing the need for adherence to IHL and ethical considerations. The ICRC report *"Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons"* (2016) addresses the legal and ethical challenges of AWS.

Similarly, the United Nations Institute for Disarmament Research (UNIDIR) has conducted extensive research on AWS, producing reports such as *"The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapon Systems and Cyber Operations"* (2017), which examines the ethical and legal dimensions of AWS. The Stockholm International Peace Research Institute (SIPRI) has also published numerous studies on the development and implications of AWS, including discussions on legal and ethical frameworks.

The United Nations Institute for Disarmament Research (UNIDIR) has conducted extensive research on AWS, producing reports such as "The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapon Systems and Cyber Operations", which examines the ethical and legal dimensions of AWS.

Several international organizations are working to address the challenges posed by AWS. The Group of Governmental Experts (GGE) on Lethal Autonomous Weapons Systems (LAWS) under the Convention on Certain Conventional Weapons (CCW) has been discussing the legal, ethical, and operational implications of AWS since 2014. In 2024, the GGE convened to continue these discussions and developed guiding principles for AWS development and use, emphasizing human control and IHL compliance. The UN Office for Disarmament Affairs (UNODA) facilitates these discussions, providing resources and support for AWS regulation (CCW, 2024).

While not specific to AWS, the Asilomar AI Principles, developed during the *Asilomar Conference on Beneficial AI* in 2017, provide guidelines for the ethical development and deployment of AI technologies, including ensuring transparency, accountability, and avoiding AI arms races (https://futureoflife.org/event/bai-2017/). The *Ethics Guidelines for Trustworthy AI*, developed by the European Commission's High-Level Expert Group on AI, emphasize ethical principles such as respect for human autonomy, prevention of harm, fairness, and explicability. Although these guidelines focus on AI broadly, they are relevant to the development and use of AWS.

National and international initiatives also contribute to addressing the ethical challenges of AWS. The *Campaign to Stop Killer Robots* (https://www.stopkillerrobots.org/), a global coalition of non-governmental organizations, advocates for a pre-emptive ban on fully autonomous weapons. This campaign emphasizes ethical concerns and stresses the importance of maintaining human control over the use of force. The *Tallinn Manual on the International Law Applicable*

to Cyber Warfare, although primarily focused on cyber operations, offers insights into how international law applies to autonomous systems, including AWS, in the context of armed conflict.

These studies, frameworks, and initiatives collectively contribute to the ongoing international dialogue on ensuring that AWS are developed and used in a manner that respects international rules of legitimacy and ethical standards. They emphasize the importance of human oversight, accountability, compliance with IHL, and minimizing harm to civilians. The international community continues to work towards establishing robust regulatory and ethical frameworks to address the complex challenges posed by AWS.

ETHICAL CONSIDERATIONS FOR AUTONOMOUS WEAPONS SYSTEMS (AWS)

The advancement of chip technology, along with aggressive gadget marketing, has intensified the technological arms race in both civilian and military sectors, leading to the advent of a new form of warfare characterized by autonomous weapons. This accelerated development has created significant disparities between technological advancements in the civilian sector across different global regions and among various military forces. If these gaps are not quickly addressed through investments in technology and strict regulations regarding their use in the civil sector, it could have unpredictable consequences. Specifically, access to these technologies by organized crime and terrorist entities could undermine global efforts in diplomacy and arms control.

Autonomous weapons systems (AWS), often referred to as lethal autonomous weapons systems (LAWS), are military systems capable of selecting and engaging targets without direct human intervention. These systems can operate based on advanced artificial intelligence algorithms and make real-time decisions on the battlefield.

Autonomous weapons systems (AWS), often referred to as lethal autonomous weapons systems (LAWS), are military systems capable of selecting and engaging targets without direct human intervention. These systems can operate based on advanced artificial intelligence algorithms and make real-time decisions on the battlefield. Such technologies may include drones, terrestrial robots, or autonomous naval and aerial systems. Autonomous weapons are designed to enhance response capabilities and combat efficiency while reducing risks for human soldiers. Their primary advantages include superior

reaction speed, the ability to operate in dangerous or inaccessible environments, and the capability to execute complex missions with increased precision. However, their use also raises numerous ethical and legal concerns, including issues related to accountability in cases of errors or misuse and their impact on international warfare norms. Just War Theory and other ethical frameworks provide moral justification for military actions, making them appear more just. Key principles such as just cause, right intention, and proportionality are essential in this regard, especially as AWS become increasingly integrated into military strategies. Global discussions surrounding these weapons focus on the need for regulation and control, as well as the potential consequences of uncontrolled proliferation of these advanced technologies.

Human judgment is crucial in military operations to ensure compliance with international humanitarian law (IHL) and to uphold ethical standards. The complexity and unpredictability of autonomous systems make it difficult to guarantee that these systems will always act within legal and ethical boundaries.

One of the fundamental ethical concerns with AWS is the potential erosion of human oversight in *life-and-death* decisions. Human judgment is crucial in military operations to ensure compliance with international humanitarian law (IHL) and to uphold ethical standards. The complexity and unpredictability of autonomous systems make it difficult to guarantee that these systems will always act within legal and ethical boundaries. Therefore, maintaining human control – particularly through *human-on-the-loop supervision* – is essential to mitigate the risks associated with autonomous decision-making. Supervisory control means having situational awareness, sufficient time to intervene, and a mechanism to take back control or deactivate the system if necessary. This mechanism could be a communication link or physical controls (ICRC, 2019).

Accountability in the use of lethal force is a cornerstone of both legal and ethical military conduct. Autonomous systems, by their nature, complicate the assignment of responsibility. If an AWS mistakenly targets civilians or commits a war crime, it is unclear who would be held accountable – the developer, the operator, or the commanding officer. This ambiguity undermines the principles of justice and accountability. Robust legal frameworks and clear lines of responsibility must be established to address these issues effectively (Cernat, 2022).

The proliferation of AWS increases the likelihood of these technologies falling into the hands of non-state actors, which could use them in ways that exacerbate conflicts and violate international norms.

This proliferation risk is compounded by the potential for these systems to be used in ways that lower the threshold for initiating conflict, as the human cost of war is perceived to be reduced. International cooperation and stringent export controls are necessary to prevent the misuse and uncontrolled spread of AWS. (ICRC, 2019).

As we look to the future, the ethical considerations surrounding AWS extend beyond immediate military applications to broader societal implications. The development and deployment of AWS must be guided by an ethical framework that prioritizes human dignity, accountability, and the preservation of peace.

The deployment of AWS raises significant ethical concerns about the dehumanization of warfare and the potential for moral disengagement. The use of robots and AI in combat may create a psychological and moral distance between decision-makers and the consequences of their actions, leading to a *"moral buffer"* effect. This detachment can result in less stringent adherence to ethical norms and a greater likelihood of collateral damage. Societal attitudes towards warfare could also shift, normalizing the use of automated systems in conflict and reducing the impetus for peaceful resolution of disputes (ICRC, 2014).

To ensure that AI algorithms used in autonomous weapons systems (AWS) respect international rules of legitimacy in military actions, several essential rules and principles must be implemented. These rules should align with international humanitarian law and ethical frameworks such as Just War Theory.

To ensure that AI algorithms used in autonomous weapons systems (AWS) respect international rules of legitimacy in military actions, several essential rules and principles must be implemented. These rules should align with international humanitarian law (IHL) and ethical frameworks such as Just War Theory. Building on the identified rules and principles, a diagram has been created to model these principles, the associated rules, and their implementation in Autonomous Weapons Systems (AWS) algorithms.

Discussions in this field are current and highly dynamic, especially with the public release of AI. The proposed model is also dynamic and must be continuously adjusted to address identified issues. It is crucial that a model of AI algorithms with standard principles should be implemented internationally, without ambiguities (United Nations, 2021).

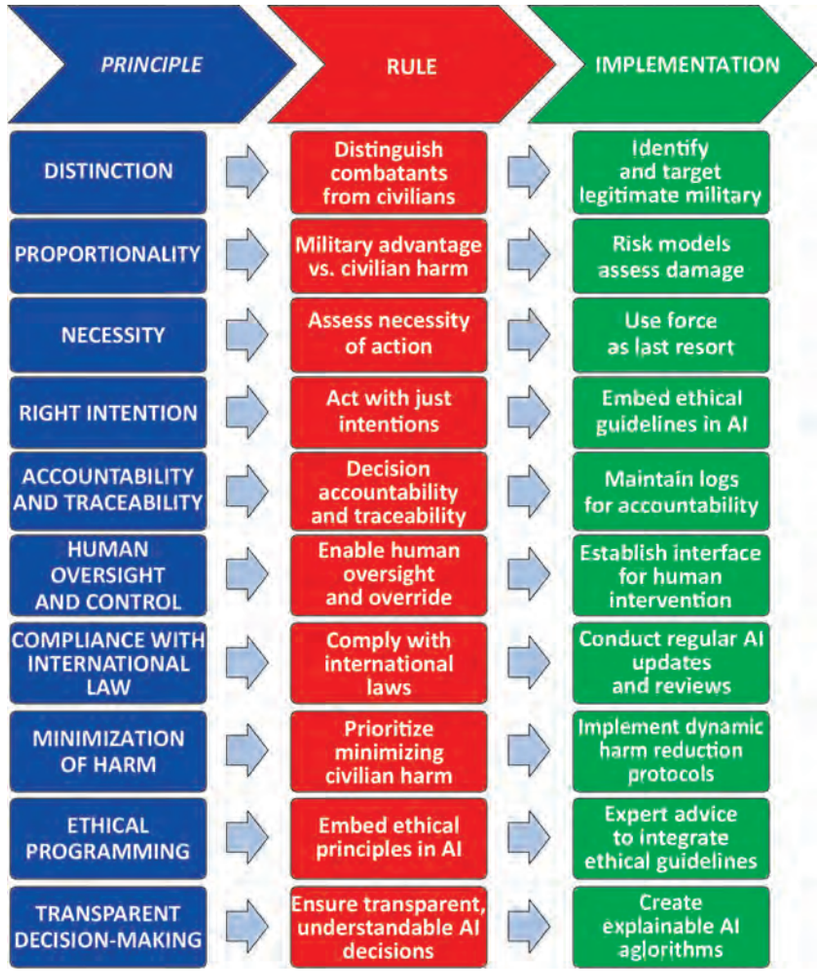


Figure 1: Model for Integrating Ethical War Principles into AI Algorithms for Autonomous Weapon Systems (authors' design)

For this model of integrating ethical war principles into AI algorithms for autonomous weapon systems, a set of moral guidelines and rules has been established to ensure that military actions are conducted in a just, humane manner, and in accordance with international laws and norms. The details of these principles, along with their application within this model, are outlined as follows:

1. **Distinction**
   - **Rule**: The AI must be able to distinguish between combatants and non-combatants, as well as between military objectives and civilian objects.

   - **Implementation**: Algorithms should include advanced object recognition and context analysis to identify and target only legitimate military targets.
2. **Proportionality**
   - **Rule**: The AI must ensure that the anticipated military advantage of an attack is not outweighed by the potential harm to civilians and civilian infrastructure.
   - **Implementation**: Algorithms should incorporate risk assessment models to evaluate potential collateral damage and avoid disproportionate use of force.
3. **Necessity**
   - **Rule**: The AI must determine whether a military action is necessary to achieve a legitimate military objective.
   - **Implementation**: Decision-making protocols should ensure that force is used only when absolutely necessary, considering all other non-violent alternatives.
4. **Right Intention**
   - **Rule**: The AI must act with the intention of achieving a just and legitimate outcome, not for malicious purposes or unnecessary harm.
   - **Implementation**: The algorithm must include validation modules for each ethical principle in the proposed model that function as checkpoints within the decision-making flow, allowing progress only if all ethical principles are respected.
5. **Accountability and Traceability**
   - **Rule**: There must be clear accountability and the ability to trace and review decisions made by AI systems.
   - **Implementation**: Logs and audit trails must be maintained, recording all decisions and actions taken by the AI for post-action analysis and accountability.
6. **Human Oversight and Control**
   - **Rule**: Human operators must have the ability to oversee and, if necessary, override AI decisions.
   - **Implementation**: Interfaces and protocols must be established to allow human intervention at critical decision points, ensuring final human judgment in the use of force.

Decision-making protocols should ensure that force is used only when absolutely necessary, considering all other non-violent alternatives.

7. **Compliance with International Law**
   - **Rule**: The AI must comply with all applicable international laws, including treaties and customary international law.
   - **Implementation**: Regular updates and reviews of AI systems must be conducted to ensure they are in line with current legal standards and norms.
8. **Minimization of Harm**
   - **Rule**: The AI must prioritize minimizing harm to civilians and civilian objects.
   - **Implementation**: Incorporate harm minimization protocols that dynamically adjust tactics to reduce potential damage and casualties.
9. **Ethical Programming**
   - **Rule**: Ethical principles should be embedded within the AI's core programming.
   - **Implementation**: Interdisciplinary collaboration involving ethicists, legal experts, and technologists to develop and integrate ethical guidelines into the AI's decision-making processes.
10. **Transparent Decision-Making**
    - **Rule**: The AI's decision-making processes must be transparent and understandable to human operators.
    - **Implementation**: Develop algorithms that provide explanations for their decisions, ensuring that human operators can understand the rationale behind actions taken by the AI.

The AI must comply with all applicable international laws, including treaties and customary international law.

Implementing these rules and principles into AI algorithms for AWS not only enhances the legitimacy of military actions involving AI but also helps to maintain international peace and security, while protecting human rights and dignity. Robust testing, continuous oversight, and regular updates are critical to maintaining the integrity and effectiveness of these AI systems in military applications.

OPTIMIZED MILITARY DECISION-MAKING PROCESS THROUGH EXTENDED REALITY (xR)

The positive impact of technological advancements on societal development is undeniable, influencing everything from recreational activities to simplifying daily tasks through their integration into everyday routines. The security sector must also evolve to meet these societal demands. Moreover, concerns regarding the ethics and legitimacy of algorithms employed in autonomous weapons systems are well-founded and require careful consideration.

The younger generation increasingly views the traditional military system as technologically outdated and lacking in job satisfaction. This perception can be addressed by leveraging their advanced technological skills, which are honed through regular interaction with gadgets and video games. By overhauling the current training system, the military can become an appealing career choice for intellectually gifted young individuals.

Furthermore, integrating advanced technologies into military training can bridge the gap between the digital proficiency of young recruits and the demands of modern military operations. This alignment can lead to a more competent and satisfied workforce, better prepared to handle the complexities of contemporary security challenges. Thus, embracing technological advancements in military training is not just beneficial but essential for creating a robust and future-ready defence system.

The US Center for Army Lessons Learned (CALL) emphasizes the importance of using wargaming in the tactical and strategic decision-making process, as outlined in the manual titled "Military Decision-Making Process".

The US Center for Army Lessons Learned (CALL) emphasizes the importance of using wargaming in the tactical and strategic decision-making process, as outlined in the manual titled *"Military Decision-Making Process"* (MDMP) (CALL, 2023). According to lessons learned over the years, war-gaming is an essential component of the MDMP, enhancing personnel effectiveness and preparedness by allowing commanders to visualize and analyse courses of action. During war-gaming, the staff examines the potential actions, reactions, and counteractions of all participants, including allied forces, enemy forces and civilians. This process facilitates the identification of strengths and weaknesses in each Course of Action (COA), leading to necessary adjustments. (Zygar, 2023)

War-gaming has been used by the US military since 1916 and has been continuously refined and integrated into training and operational programmes to adapt to new requirements and technologies. Over the decades, simulation methods have evolved from maps and physical pieces to complex digital simulations, providing an increased level of realism and detail. These improvements have allowed the military to more accurately anticipate enemy reactions and develop more effective strategies.

In recent years, Extended Reality (xR) technologies, which include Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR), have also been incorporated into military training. These technologies create immersive environments where trainees can engage in realistic 3D simulations, such as piloting aircraft or performing medical procedures, thus reducing real-world risks. xR enhances the visualization of the battlefield, allowing for detailed views of terrain, enemy positions, and potential hazards. Additionally, xR supports real-time, collaborative planning sessions with geographically dispersed teams, ensuring that all relevant stakeholders can contribute to the decision-making process. This integration of xR technologies into wargaming and other training methods has further improved the effectiveness and readiness of military personnel (Freedman, 2019).

xR supports real-time, collaborative planning sessions with geographically dispersed teams, ensuring that all relevant stakeholders can contribute to the decision-making process. This integration of xR technologies into wargaming and other training methods has further improved the effectiveness and readiness of military personnel.

One argument in favour of this technological adaptation is the potential for enhanced engagement through the use of digital extended reality technologies. These technologies can revolutionize training programmes by providing diverse and immersive learning methods, such as interactive lessons, modules, and personalized training sessions. This approach makes learning not only more engaging but also more effective, as it caters to individual learning styles and needs.

According to the *Cone of Learning* developed by Edgar Dale in 1946, also known as the *Cone of Experience* (Growth, 2024), the human brain retains more information by what they *"do"* as opposed to what they *"hear", "read"*, or *"observe"*.

The *Cone of Learning* emphasizes the importance of active participation and experiential learning. According to Dale, engaging multiple senses while actively participating in the learning process leads to better retention and understanding. Utilizing Extended Reality

(xR) technologies can effectively create these immersive and interactive learning environments. This approach aligns with Dale's principles, enhancing retention and understanding by engaging multiple senses and facilitating active participation.

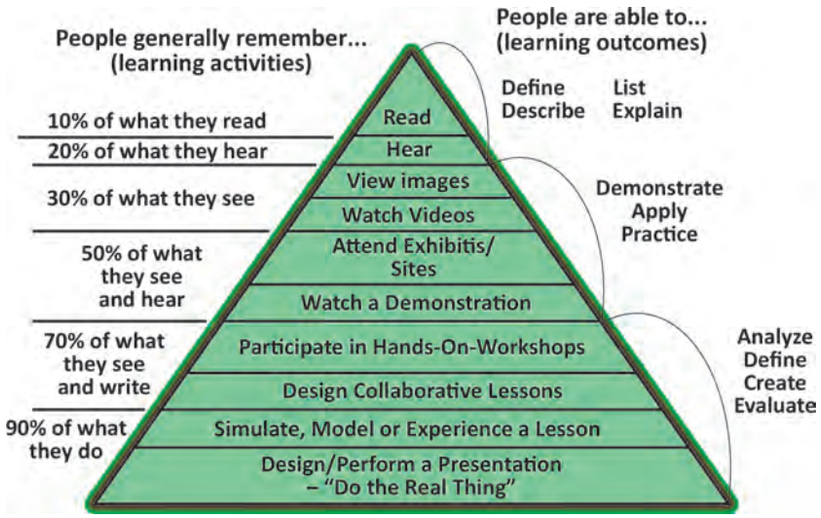


Figure 2: Cone of Learning example
(https://commons.wikimedia.org/wiki/File:Edgar_Dale%27s_cone_of_learning.png, Jeffrey Anderson)

Moreover, xR can integrate data from various sources (e.g., drones, satellites, ground reports) in real time, providing a comprehensive operational picture. This data-rich environment supports more accurate and legitimate decision-making. Continuous training using xR can help military personnel to quickly adapt to new technologies and tactics, ensuring that they are always operating at peak efficiency and effectiveness.

However, over-reliance on xR technology could lead to vulnerabilities. If the technology fails (due to cyber-attacks or technical issues), decision-making processes could be severely disrupted. The immersive nature of xR can sometimes lead to cognitive overload, where the sheer amount of information available can overwhelm decision-makers, potentially leading to poor decisions.

Over-reliance on xR technology could lead to vulnerabilities. If the technology fails (due to cyber-attacks or technical issues), decision-making processes could be severely disrupted.

While xR can simulate many scenarios, it can never fully replicate the complexities and unpredictability of real-life situations.

Overconfidence in simulated outcomes might lead to decisions that are not well-suited for actual conditions. The scenarios and data used in xR simulations can be biased based on the inputs and design choices. It could lead to skewed perceptions and potentially illegitimate decisions if not carefully managed.

The use of Extended Reality (xR) enhances the decision-making process and bolsters the legitimacy of military actions through realistic simulations and comprehensive data integration. As a valuable tool in modern military decision-making, xR can improve the legitimacy and effectiveness of military operations in the context of current technological advancements. However, excessive reliance on this technology may lead to ethical concerns and operational risks.

As a valuable tool in modern military decision-making, xR can improve the legitimacy and effectiveness of military operations in the context of current technological advancements.

CONCLUSIONS

The study highlights a significant transformation in modern warfare driven by technological advancements such as artificial intelligence (AI), autonomous weapon systems (AWS), and virtual reality (VR) training.

On the one hand, while these technologies can enhance precision and operational effectiveness, they simultaneously present ethical and legal challenges that require careful management. The analysis emphasizes the potential erosion of responsibility and accountability as decision-making processes shift from humans to algorithms, which can lead to a detachment from the consequences of military actions, potentially resulting in unjustified actions and an increase in civilian casualties.

Illustrating the complexity of balancing technological capabilities with ethical obligations, the use of AI in Israeli military operations in Gaza demonstrates the necessity for robust legal frameworks and clear lines of responsibility. The AI-based *"Lavender"* system, which led to significant collateral damage, underscores this crucial point.

It is imperative to maintain human oversight and control over autonomous systems to mitigate risks and uphold ethical standards. AI algorithms for AWS must incorporate principles such as distinction, proportionality, necessity, and accountability to align with ethical and legal norms. The model for integrating the principles of the ethics

of war into AI algorithms for autonomous weapon systems, as presented in the study, proposes the use of regulatory frameworks that include continuous verification of algorithmic decisions through simulations and complex scenarios to ensure compliance with rules of engagement and international laws of armed conflict. This model emphasizes the importance of transparency and auditability in the development and implementation of AI, so that any decision made by autonomous systems can be reviewed and validated by human decision-makers.

International efforts, including frameworks developed by the International Committee of the Red Cross and the United Nations Institute for Disarmament Research, are essential in addressing the ethical and legal challenges associated with AWS. These initiatives aim to establish guidelines for the responsible use of advanced military technologies, protecting civilian lives and promoting justice.

The integration of technological advancements in warfare requires a nuanced approach that balances operational advantages with ethical and humanitarian obligations. Continuous research, international cooperation and stringent regulation are imperative for navigating the complexities of modern warfare, ensuring that technological progress does not compromise human rights and international stability.

ROMANIAN MILITARY THINKING

The model for integrating the principles of the ethics of war into AI algorithms for autonomous weapon systems, as presented in the study, proposes the use of regulatory frameworks that include continuous verification of algorithmic decisions through simulations and complex scenarios to ensure compliance with rules of engagement and international laws of armed conflict.

BIBLIOGRAPHY:

1. Arkin, R. (2009). *Governing Lethal Behavior in Autonomous Robots.* New York: CRC Press.
2. Bendett, S. (2022). *The Role of Iranian-Made Shahed-136 Drones in Russian Military Strategy*. In *Journal of Strategic Studies*, pp. 489-510.
3. Center for Army Lessons Learned (CALL). (2023). *Military Decision – Making Process organizing and conducting planning*, US Army: https://api.army.mil/e2/c/downloads/2023/11/17/f7177a3c/23-07-594-military-decision-making-process-nov-23-public.pdf, retrieved on 10 May 2024.
4. Cernat, R. (2022). *Sistemele de arme autonome letale – tehnologie emergentă și potențial nimicitoare*. In Romanian Military Thinking International Conference Proceedings, pp. 156 -174.
5. Chatelier, P.R., Seidel, R. (2013). *Virtual Reality, Training's Future? Perspectives on Virtual Reality and Related Emerging Technologies.* Germany: Springer.

6. Convention on Certain Conventional Weapons/CCW (2024). *Group of Governmental Experts of the High Contracting Parties related to emerging technologies in the area of lethal autonomous weapons systems (LAWS),* UNODA, https://meetings.unoda.org/ccw-/convention-on-certain-conventional-weapons-group-of-governmental-experts-on-lethal-autonomous-weapons-systems-2024, retrieved on 20 May 2023.
7. Dombe, A.R. (February 2023). *Commander of the Artificial Intelligence Center, 8200: Artificial intelligence enables faster classification and detection of terrorist targets*, Israel Defense Web: www.israeldefense.co.il/node/57256#google_vignette, retrieved on 15 April 2024.
8. Freedman, J. (2019). *Using VR in the Military.* United Kingdom: Cavendish Square.
9. Galeotti, M. (2023). *Drone Warfare and the Russian Military: Lessons from the Ukraine Conflict*. In *Military Review*, pp. 112-126.
10. Growth (2024), https://www.growthengineering.co.uk/what-is-edgar-dales-cone-of-experience, retrieved on 22 May 2024.
11. ICRC (2019). *Autonomy, Artificial Intelligence and Robotics: Technical Aspects of Human Control,* pp. 2-9, https://www.icrc.org/sites/default/files/document/file_list/autonomy_artificial_intelligence_and_robotics.pdf, retrieved on 10 April 2024.
12. ICRC. (1977). *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 51(5)(b), art. 57.* International Humanitarian Law Databases, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977, retrieved on 10 March 2024.
13. ICRC (26-28 March 2014). *Report of the ICRC Expert Meeting on 'Autonomous weapon systems: technical, military, legal and humanitarian aspects'.* Geneva, https://www.icrc.org/sites/default/files/external/doc/en/assets/files/2014/expert-meeting-autonomous-weapons-icrc-report-2014-05-09.pdf, retrieved on 20 April 2024.
14. IEEE SA. (n.d.). *IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. „Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, First Edition"*, https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead1e.pdf., retrieved on 12 March 2024.
15. Rojansky, M., Kofman, M. (2022). *The Impact of Technological Integration on Russian Military Tactics in Ukraine*. In *Foreign Affairs*, pp. 67-84.
16. Scharre, P. (2018). *Army of None: Autonomous Weapons and the Future of War.* New York: W.W. Norton.

17. Scharre, P. (2018). *Autonomous Weapons and Operational Risk*. In *The Ethics of Autonomous Weapons*, pp. 23-399. New York: Oxford University Press.
18. Singer, P.W. (2009). *Wired for War: The Robotics Revolution and Conflict in the 21st Century.* New York: Penguin Press.
19. United Nations (2021). *Lethal Autonomous Weapon Systems: Legal, Ethical, and Operational Issues.* New York: United Nations.
20. Walsh, T. (2018). *Machines That Think: The Future of Artificial Intelligence.* New York: Prometheus Books.
21. Walzer, M. (2006). *Just and Unjust Wars: A Moral Argument with Historical Illustrations.* Basic Books.
22. Warrick, J. (2022). *From Theory to Practice: The Real-Time Implementation of Drone Warfare Tactics in Ukraine*. In *The Washington Quarterly*, pp. 93-109.
23. Williams, A. (2021). *Autonomous Systems: Legal and Ethical Challenges.* New York: Routledge.
24. Yuval, A. (2024). *'Lavender': The AI machine directing Israel's bombing spree in Gaza,* https://www.972mag.com:https://www.972mag.com/lavender-ai-israeli-army-gaza/, retrieved on 15 April 2024.
25. Zygar, M. (2023). *Adapting to the Battlefield: The Evolution of Russian Military Strategy in the Face of Technological Change*. In *International Journal of Military History and Historiography*, pp. 75-94.
26. https://futureoflife.org/event/bai-2017/. *Beneficial AI 2017*, retrieved on 12 June 2024.
27. https://commons.wikimedia.org/wiki/File:Edgar_Dale%27s_cone_of_learning.png, Jeffrey Anderson, retrieved on 12 June 2024.
28. https://www.stopkillerrobots.org/; https://una.org.uk/what-we-do/campaign-stop-killer-robots, retrieved on 12 June 2024.

NUCLEAR THREAT – THE FACTOR THAT LESSENED THE LIKELIHOOD OF CONFLICT ESCALATION DURING THE COLD WAR –

Lieutenant Colonel Associate Professor Andi Mihail BĂNCILĂ, PhD

"Ferdinand I" Military Technical Academy, Bucharest

10.55535/RMT.2024.3.12

The nuclear weapon, the "ambassador" of peace, is one of the strangest ideas ever uttered. Despite the obvious nonsense, this concept can be considered a great truth. Blinded by concerns to find the most effective method of winning the bipolar confrontation, the two superpowers of the 20th century, the USA and the USSR, undertook the most extreme and most expensive experiments to put them at an advantage.

After defusing the tension of the situation created as a result of the deployment of nuclear missiles on the territory of Turkey and Cuba, the two superpowers engaged in an extensive process of disarmament, which also involved representatives of the academic environment, who expressed their positions and offered solutions to the problems about which the two superpowers continued to have reservations.

Keywords: nuclear weapon; Cold War; USSR; USA; crisis;

TECHNOLOGICAL EQUALITY – I.V. STALIN'S GREAT DREAM

The end of the Second World War caused, as expected, a split within the coalition formed during the conflict between the US, the UK, France, and the USSR to carry out armed actions against the Axis powers. Even if the need for the moment justified the creation of that group of forces, the ideological position of the democratic states could not be aligned with the communist ideology promoted by the Soviets. As a result, the former *"allies"* became declared enemies who built alliances and developed military strategies to achieve a total victory in the ideological confrontation unfolded over half a century. One of the most important aspects of the new type of conflict was the desire of the two configured superpowers – USA and USSR – to build a military instrument through which they could gain a major advantage, in strategic terms, over the opponent. The creation of the atomic weapon and its successful use against Japan positioned the USA as the main systemic power. It was a great advantage in the first part of the confrontation, which was intended to be promoted as the main deterrent of the USSR.

The creation of the atomic weapon and its successful use against Japan positioned the USA as the main systemic power. It was a great advantage in the first part of the confrontation, which was intended to be promoted as the main deterrent of the USSR.

Enthusiastic about the security provided by the atomic weapon, American policymakers neglected the USSR's efforts to achieve parity in military capabilities. The existence of the nuclear weapon in the arsenal of the American military was seen as a guarantee of almost certain victory. Thus, many of the American politicians almost dared to ignore the judgments of military strategy (Gray, 2010, p. 227). Aware of the fact that, with the emergence of the new weapon, the numerical superiority of the Soviet armed forces was nullified, the leader of the USSR, Joseph Vissarionovich Stalin, ordered the start of a nuclear armament programme. Despite his optimistic approach and his defiant statements like: *"Atomic bombs are intended to frighten the weak-minded, but they cannot decide the fate of a war"* (Sixsmith, 2021, p. 389), he was willing to spare no effort to nullify the US strategic advantage.

Aware of the risks arising from the expansion of the group of states possessing nuclear technology, the USA submitted a report to the UN expressing its agreement to bring nuclear technology under the control of this organization. The American request came in the form of a plan for the control of atomic energy, bearing the name of its initiator, Bernard Mannes Baruch, an adviser to President F.D. Roosevelt. He requested the establishment of the Atomic Energy Commission.

Aware of the risks arising from the expansion of the group of states possessing nuclear technology, the USA submitted a report to the UN expressing its agreement to bring nuclear technology under the control of this organization (Townshend, 1997, p. 141). The American request came in the form of a plan for the control of atomic energy, bearing the name of its initiator, Bernard Mannes Baruch, an adviser to President F.D. Roosevelt. He requested the establishment of the Atomic Energy Commission (Buck, p. 1), which would then regulate access to nuclear technology and implicitly to the manufacture of atomic weapons. To the USSR, such a prospect seemed unacceptable, and they were willing to risk everything, including exclusion from the international community, to achieve a status similar to that of the USA. As a result, the Soviet representative at the UN refused to sign the protocol proposed by the Americans. Moreover, the leader of the USSR, I.V. Stalin, considered that approach as an attempt by the Americans to prohibit the Soviets from achieving the much-desired *"technological equality"* (Gray, p. 228), in order to later impose their own system of thought on them.

The first Soviet efforts to create an atomic weapon had begun in the early 1930s, but, because of the purges ordered by I.V. Stalin, many researchers had died or been imprisoned in camps, thus halting the Soviet nuclear programme. During the course of the war, the Soviet dictator was constantly informed about the advance made by the Westerners in the development of their nuclear programme. In 1943, the information received clearly indicated that the Americans were going to achieve the much-desired weapon, which led I.V. Stalin to relaunch the nuclear research programme. The great Russian physicist Igor Kurchatov was appointed to lead the group of Soviet scientists, who was promised all possible support (Johnson, 2019, p. 22). In the meeting he held with Russian scientists immediately after the Hiroshima bombing, I.V. Stalin mentioned the immediate need to obtain the atomic weapon: *"One request from you, comrades, is to supply us with atomic weapons as soon as possible. The balance has been destroyed. Give your bomb – it will remove a great danger to us. Ask for whatever you want, comrades! You will not be refused! As the saying goes, until the child cries, the mother does not give him the breast"*. (Holloway, 1981, p. 183). The restriction of the study to some authors considered *"bourgeois"* greatly hampered the mission of the scholars who personally informed I.V. Stalin that they could not develop the research without having access to Einstein's theory of relativity. The dictator approved their approach by ordering to Lavrentiy Pavlovich Beria, head of the feared People's Commissariat for Internal Affairs (NKVD) repression service, to provide them with everything they wanted, also mentioning the fact: *"Leave them alone – we can always shoot them later!"* (Sixsmith, p. 392). The mission of the Soviet researchers was greatly simplified by the action of Ethel and Julius Rosenberg, who, for ideological reasons, chose to deliver to the Soviets important documents containing the significant details for the production of such devices (Garber, Walkowitz, 1995, p. 2).

On 29 August 1949, at the Semipalatinsk range, in Kazakhstan SSR, the USSR detonated its first nuclear weapon, with a capacity of 22 kilotons, similar to the famous "Fat Man", used by the USA in Nagasaki, thereby nullifying the United States' nuclear advantage. From that moment on, the two superpowers embarked on an extensive nuclear weapons programme.

The American monopoly on the production of nuclear weapons ended much faster than expected during the war. *"Miraculously"* just four years after the end of the war, on 29 August 1949, at the Semipalatinsk range, in Kazakhstan SSR, the USSR detonated its first nuclear weapon, with a capacity of 22 kilotons, similar to the famous *"Fat Man"*, used by the USA in Nagasaki (Podvig, 2004, p. 2), thereby nullifying the United States' nuclear advantage. From that moment on, the two superpowers embarked on an extensive nuclear weapons programme. The mentioned fact has severely tested the ability of the international community to effectively manage such a situation and to find solutions leading to détente in terms of the political situation between the two states. After obtaining the first atomic weapon, the Soviets started an extensive programme aimed at creating devices for transporting such weapons. The first vector capable of carrying a nuclear payload was made even before the advent of nuclear weapons, in 1946. The TU-4 (Tupolev) aircraft, which was a faithful copy of the American model B-29, became the pride of Soviet aviation. However, taking into account the very small range, it could not cause problems for the USA. The programme continued at a rapid pace, which allowed two more TU-16 and TU-20 aircraft to be developed in an interval of only 10 years. Those far more powerful devices with a range of 3,800 miles (Townshend, p. 142), were capable of reaching the American coastline. The big problem that the Soviets had to deal with was that, at that time, there was no possibility that those devices could be supplied from the air. As a result, those aircraft could not have returned to Soviet territory, which again would have discouraged

any of the pilots from accepting such a mission. Consequently, the Soviets paid increased attention to the creation and development of strategic missiles capable of hitting any target on the US territory. In this regard, the Russians unjustifiably benefitted from a major advantage in relation to their competitor. At that time very few specialists knew that at the end of the war the USSR had captured a large part of the German scientists who had been involved in the Nazi missile programme. Despite the fact that the director of the German rocket development project, Wernher von Braun, had been arrested by the Americans and sent to the USA, the Soviets had captured the laboratories and factories where the German scientists had been working, thus taking over most of the results of their work, including prototypes of rockets (Bergaust, 2017, p. 119). The first Soviet ballistic missiles were obtained in 1955, while the Americans achieved them three years later, having a serious problem regarding the insufficient range of only 2,500 kilometres (Townshend, ib.). By the early 1960s the two superpowers had greatly diversified their nuclear payload capabilities, being able to easily strike any type of target at close range.

The first Soviet ballistic missiles were obtained in 1955, while the Americans achieved them three years later, having a serious problem regarding the insufficient range of only 2,500 kilometres.

THREATS AND NUCLEAR CRISES IN THE EARLY COLD WAR

The first tense moment of the Cold War was the dispute over the control of the German capital Berlin, which took place during the years 1948-1949. The unpredictability of the Soviets in terms of the way of action led the Americans to also consider the use of the nuclear arsenal as a backup option. During the hostilities caused by the Soviet blockade of West Berlin, taking advantage of the uniqueness of its nuclear power, the USA tried to intimidate the USSR by sending two B-29 squadrons to Europe. Even though the configuration of their devices was similar to those that bombed Nagasaki and Hiroshima, there was no confirmation that they were accompanied by atomic weapons. Considering that the Soviet nuclear programme had not yet delivered the first atomic weapon, there were voices that claimed that the deployment of those aircraft decisively influenced the Soviet decision to abandon the blockade (Dingman, p. 54). The aspect was highlighted even by the US President, Harry S. Truman, who stated: *"If it weren't for Bomb, the Russians would have taken control of Europe a long time ago"* (Gaddis, 2021, p. 57).

The advance of research in the field of nuclear weapons production was evident as both superpowers developed several types of such devices that could be used in different phases of the armed conflict. Perhaps the most dangerous in terms of ease of use was the tactical nuclear weapon. It was intended to be used directly on the battlefield against large military groups whose annihilation was becoming imperative. The first discussions about the possibility of using such weapons were held on 25 June 1950 when President Truman requested the advice of the Air Force Chief of Staff, Hoyt S. Vandenberg, to develop an action plan that would analyse the possibility to annihilate the Soviet military bases located near the Korean peninsula using atomic weapons (Dingman, p. 55).

The tensest moment of the first part of the Cold War occurred in November 1950, when the American troops led by General Douglas MacArthur advanced quickly into the territory of North Korea, reaching the banks of the Yalu River at the border with China. His action was based on the intelligence according to which, at the urging of Stalin, the Chinese dictator, Mao Zedong, made the decision to send troops to support the Korean communists: *"We should not miss the attempt to help the Koreans (...), we must give them a hand of help by sending there volunteers from among our soldiers"* (Gaddis, p. 47). As early as early August, Mao had ordered General Gao Gang, the commander and political commissar of the Northeast Military District, to form a task force of over 250,000 men near the Korean border (Chen, 1992, p. 12). The advance of American forces was also halted because of the pressure exercised by the 300,000 *"Chinese volunteers"* who had been crossing the river since 26 November. In that context, D. MacArthur asked President H. Truman for approval to use five tactical nuclear weapons to stop their advance. According to calculations, the use of those weapons could have caused the loss of over 150,000 Chinese military, which contributed decisively to the cessation of hostilities. What the US General took into account was Mao's determination to continue the offensive regardless of the cost in human lives.

The advance of research in the field of nuclear weapons production was evident as both superpowers developed several types of such devices that could be used in different phases of the armed conflict. Perhaps the most dangerous in terms of ease of use was the tactical nuclear weapon.

The situation was further complicated when the Chinese asked the Soviets to use their own nuclear weapons in case the Americans decided to bomb the Chinese troops in Korea. On 2 December, the USSR submitted an ultimatum to the USA demanding the cessation

of any initiative to use nuclear weapons. Moreover, to show their determination, on 4 December, they ordered the lifting of two nuclear-armed bombers from the base in Vladivostok, which had the mission to bomb the US troops stationed at Pusan and Inchon. Ignoring the Soviet warning, MacArthur escalated and ordered the bombers stationed in Japan to attack Vladivostok as well as the Chinese cities of Shenyang and Harbin (Gaddis, p. 52). The situation was de-escalated only as a result of an exemplary mobilization of the international community that, aware of the risk, asked the USA to abandon General MacArthur's crazy plans. Following those protests and the rational calculations that were made by US politicians in April 1951, President H. Truman decided to remove General MacArthur from office. The decision to dismiss the general was one of the most unpopular decisions made by President H. Truman who argued his point of view that if it had not happened the world would have been headed for the Third World War: *"I thought a lot about it and finally decided that there were times when he wasn't exactly in his head. And there was never anyone around him to keep him in line. (…). Why the hell, if he had his way, he'd take us into World War III and blow up two-thirds of the world".* (Time, 1973).

After the death of the Soviet dictator, Joseph Vissarionovich Stalin, in 1953, one of his trusted men, the former political commissar, the hero of Stalingrad, Nikita Khrushchev, was promoted to the leadership of the USSR. Stalin's successor tried to recommend himself as the "reformist" leader of the USSR, who wanted to rebalance the country after the "great Stalinist terror".

THE 1962 CUBAN MISSILE CRISIS

After the death of the Soviet dictator, Joseph Vissarionovich Stalin, in 1953, one of his trusted men, the former political commissar, the hero of Stalingrad, Nikita Khrushchev, was promoted to the leadership of the USSR. Stalin's successor tried to recommend himself as the *"reformist"* leader of the USSR, who wanted to rebalance the country after the *"great Stalinist terror"*. At the beginning of his tenure at the head of the CPSU, he initiated several discussions with American leaders, discussions that naturally addressed the nuclear weapons programme. For a moment the world seemed to return to a balance in the escalating conflict between the two great powers. The leaders of the two superpowers simulated the possibility of reaching an agreement regarding nuclear weapons. They agreed to organize an international conference to defuse the growing tension. The meeting was held in Geneva on 18 July 1955 (Draft Treaty on European Security, 1955). The desire of all participants was to provide concrete solutions

to the problems facing the bipolar world. At that time, the discussions held there were viewed with optimism, the international community considering the event as the solution that could lead to the detente in the Soviet-American relations.

Unfortunately, Nikita Khrushchev was not very interested in the subject. In fact, he wanted to hide from the world his plan to reorganize the internal policy of the Soviet state, a policy that remained known as *"de-Stalinization",* using that diversion. He promoted the false idea that he would reject the cult of personality and would like to return to the principles of collective leadership (Băncilă, 2015, p. 193). In fact, all those supposed reforms masked his energetic actions to eliminate his political opponents. Like his predecessors, V.I. Lenin and I.V. Stalin, N. Khrushchev devised a plan to discredit his candidates, the process of de-Stalinization serving him well to force them into exile or even sentence them to death. One of the most dangerous opponents, Lavrentiy Pavlovich Beria, was accused of treason, terrorism and counter-revolutionary activity and sentenced to death (Knight, 1993, p. 192). Once his power was consolidated, N. Khrushchev devoted himself to foreign policy, through which he tried to increase the prestige and influence of the USSR in the world. His nuclear programme remained a priority. Thus, he became the protagonist of the tensest moment of the Cold War, the Cuban Missile Crisis.

ROMANIAN MILITARY THINKING

In spite of the international commitments made by N. Khrushchev, he never ceased to use nuclear terror to intimidate the ideological opponent. The greatest challenge of the Cold War occurred on 14 October 1962, when a U-2 operated by the US Air Force flew over the airspace of the island of Cuba and identified on its territory several launch pads for Soviet medium-range missiles.

In spite of the international commitments made by N. Khrushchev, he never ceased to use nuclear terror to intimidate the ideological opponent. The greatest challenge of the Cold War occurred on 14 October 1962, when a U-2 operated by the US Air Force flew over the airspace of the island of Cuba and identified on its territory several launch pads for Soviet medium-range missiles. The crisis lasted until 20 November 1962, and raised the military alert level of the USA and its allies to the highest level of the entire Cold War period. According to the calculations of the US President, John F. Kennedy, the probability of breaking out a total war between the two superpowers was 50% (Dobbs, 2008, p. 251).

Taking into account that at the beginning of the 1960s there was no technology necessary to intercept the enemy's missiles, the probability of avoiding a nuclear disaster was minimal. According to the plans made at the highest level of the leadership of the two states,

it was desirable that when one of them would have taken the decision to initiate nuclear bombings, it would have the possibility to totally annihilate the capabilities of the opponent, otherwise risking its own self-destruction. In his book, *"Geopolitics and Geostrategy"*, Paul Claval mentioned that Georgy Malenkov, Prime Minister of the USSR between 1953 and 1955, stated that: *"a nuclear conflict could have such consequences for the country that initiates it that victory would lose its meaning".* (Claval, 2001, p. 108). The analysis continued to dominate the foreign policy of the two states, each of them weighing any situation that could have escalated to a nuclear conflict.

At the time of the outbreak of the Cuban Missile Crisis, the two countries had made significant progress in the construction of nuclear missile submarines. Each of the two adversaries possessed several dozen of such devices that could remain submerged even for several months, during which time they could move undetected to a sufficiently small distance from the target (Ib., p. 109). Even if all the land targets were initially hit, the undetected submarines could in turn eliminate a large part of the targets in the enemy territory.

Each missile could carry between 6 and 15 nuclear warheads that could hit different targets and could be launched from the depths of the planetary ocean from the submarines of the two states. These vectors carrying nuclear weapons had the ability to move without much difficulty on about 70% of the planet's surface, their location being particularly difficult to detect.

The most important problem that should have been managed, however, arose when both powers developed multiple warhead missiles. Each missile could carry between 6 and 15 nuclear warheads that could hit different targets and could be launched from the depths of the planetary ocean from the submarines of the two states (Tămaș, 1999, p. 205). These vectors carrying nuclear weapons had the ability to move without much difficulty on about 70% of the planet's surface, their location being particularly difficult to detect.

CONCERNS OF CIVIL SOCIETY AND ACADEMIA FOR THE RESOLUTION OF THE NUCLEAR CRISIS

After the end of the *Cuban Missile Crisis*, the two superpowers started a series of discussions regarding the identification of the optimal solution to reduce the nuclear arsenal and to compel other states to give up their nuclear programmes. The first step was taken in 1963 when, through the signed treaty, the two agreed to give up surface tests (Kissinger, 2015, p. 239). Subsequent discussions led to new commitments that materialized in 1968 with the signing of the Nuclear Non-Proliferation Treaty (Ib., p. 271), to which Great

Britain also joined. The other two nuclear powers recognized at that time, China and France, signed the treaty in 1992, and a number of states such as India and Pakistan categorically refused to sign it. The two superpowers pledged to support the world's states to develop their civilian nuclear programmes in exchange for signing the treaty. An unprecedented situation was created by North Korea which, after initially agreeing to sign the agreement, withdrew in 2003 and developed its nuclear weapons programme, which it successfully completed in 2006 by detonating its first nuclear bomb. Despite this failure, the treaty contributed significantly to reducing the number of nuclear powers, states such as Iraq, Syria, Iran, South Africa, Brazil or Argentina being stopped from continuing their nuclear programmes (Ib., p. 272).

The possibility of attacks on large urban agglomerations has led the states of the world to identify solutions to reduce the possible loss of human life. The political class and civil society have laid the foundations for a long-term relationship based on mutual respect and the achievement of common goals (Ib., p. 239). During the 1950-1960 period, in the American academic environment (Harvard, Caltech, MIT universities), there were several meetings in which the development of a doctrine of the *"limited use"* of atomic weapons was discussed (Ib., p. 268). It was proposed that they would be used only on the battlefield or that they would engage exclusively military targets.

In 1983, the American astronomer Carl Sagan developed a theory of the disaster that could affect Terra in the event of a nuclear war. He claimed that the huge amount of dust and smoke that would have been released into the atmosphere could have absorbed almost 99% of the sun's brightness, thus producing a true nuclear winter.

All these elements created a state of tension at the societal level. Thus, atomic weapons ceased to represent only a preoccupation of the military and political decision-makers. Many academics began to promote pacifist ideas and made calculations that attempted to determine the effects that a nuclear war might produce. In 1983, the American astronomer Carl Sagan developed a theory of the disaster that could affect Terra in the event of a nuclear war. He claimed that the huge amount of dust and smoke that would have been released into the atmosphere could have absorbed almost 99% of the sun's brightness, thus producing a true nuclear winter. The calculated interval of lack of sunlight, between 6 months and 2 years, would not have been the only effect created. There was talk of radioactive contamination, acid rain, destruction of the ozone layer and many other problems that initially could have led to the extinction of plants and animals and later humans (Sagan, Pollack, Ackerman, Toon, Turco, 1983, pp. 1283-1292).

In 1981, the Home Office simulated the possible consequences of a nuclear attack on Great Britain. In the first 15 days after the Soviet attack occurred, 45.3 million people could have died, and other 3 million would have been seriously injured. Similar calculations were made in the USA, which estimated that in the event of an attack by the USSR, at least 100 million people could have died (Claval, ib., p. 109). This type of analysis produced the expected result and led the political people in the governance of the two superpowers to be cautious and analyse very carefully any of the situations that could have led to such a catastrophe.

The two superpowers disputing their primacy within the system were required to negotiate to identify solutions that would avoid nuclear winter. Despite the unpredictability that continued to dominate the relations between the two political-military blocs and to back up the arms race, political leaders were willing to negotiate.

Another important contributor to the securing of atomic weapons was the political scientist Francis Fukuyama who spoke of the solidarity of the two major nuclear powers (Fukuyama, 2007), coining the term *"political prudence".* He insisted on increasing the level of collaboration between the politicians of the two states with the objective of identifying solutions capable of limiting proliferation and reducing the number of nuclear warheads in use. More than ever in history, the two superpowers disputing their primacy within the system were required to negotiate to identify solutions that would avoid nuclear winter. Despite the unpredictability that continued to dominate the relations between the two political-military blocs and to back up the arms race, political leaders were willing to negotiate. Unexpectedly, that strategy created exactly the opposite effect, the nuclear threat, based on the principle of producing massive damage, deterred the use of such devices and also prevented the outbreak of a classic conflict. This effect produced especially on the psychological level has remained known in history as *nuclear peace*. The only leader who was not intimidated by the weapons of the two superpowers was Mao Zedong who declared that the state he led was prepared to sacrifice even a few million lives in exchange for preserving political independence (Harris, 1965, p. 90).

CONCLUSIONS

Despite all the commitments made and the possible risks that would have resulted from a nuclear war, the two superpowers continued to allocate significant sums of money to their nuclear programmes and to accumulate numerous devices. In 1991, at the end of the Cold War, it was estimated that the two superpowers together possessed approximately 20,000 nuclear warheads (USSR – 9,537 and USA – 8,772) (Ib., p. 112), a legacy that created numerous problems in the years that followed. Nuclear weapons in use or in stock had to be maintained and guarded, which posed financial problems for the Russian Federation and the other successor states of the USSR on whose territory such weapons remained stored. Even if the political leadership of those states had assumed through international treaties the limitation of the nuclear arsenal and the possibility of using it, there was no guarantee that those devices could have fallen into the hands of terrorist groups. This type of threat had not been taken into account until that moment, but in the new international system created, non-state actors had become the equals of nation states.

Moreover, after the attack of the Russian Federation on Ukraine, on 24 February, 2022, the world has been once again faced with a new Cold War. The outbreak of the crisis in Ukraine and the military impasse in which the Russian leadership has entered have brought the *"nuclear solution"* back to the attention of political decision-makers. Several times during the course of hostilities, the Russian Federation has set *"red lines"* and expressed its intention to use nuclear weapons. Using the experience resulting from the previous confrontations in which the use of the nuclear bomb was discussed, I believe that the international community will find the optimal solution that will defuse this crisis and the nuclear option will still remain a deterrent.

ROMANIAN MILITARY THINKING

Nuclear weapons in use or in stock had to be maintained and guarded, which posed financial problems for the Russian Federation and the other successor states of the USSR on whose territory such weapons remained stored. Even if the political leadership of those states had assumed through international treaties the limitation of the nuclear arsenal and the possibility of using it, there was no guarantee that those devices could have fallen into the hands of terrorist groups.

BIBLIOGRAPHY:

1. Băncilă, A.M. (2015). *România în Consiliul de Ajutor Economic Reciproc, de la dictat economic la emancipare. 1949-1964*. București: Editura Ars Docendi.
2. Bergaust, E. (2017). *Wernher von Braun*. New York: Stackpole Books.
3. Buck, A. *A history of Atomic Energy Commission*, p. 1, https://www.osti.gov/servlets/purl/5977409, retrieved on 15 March 2024.
4. Chen, J. (1992). *China's Changing Aims during the Korean War, 1950-1951*. In *The Journal of American-East Asian Relations*, vol. 1, no. 1, JSTOR, http://www.jstor.org/stable/23613365, retrieved on 19 April 2024.
5. Claval, P. (2001). *Geopolitică și geostrategie. Gândirea politică, spațiul și teritoriul în secolul al XX-lea*. București: Editura Corint.

6. Dingman, R. (1988/1989). *Atomic diplomacy during the Korean War*. In *International Security*, vol. 13, no. 3, Winter, https://www.jstor.org/stable/2538736?read-now=1&seq=1#page_scan_tab_contents, retrieved on 18 April 2024.
7. Dobbs, M. (2008). *One Minute to Midnight: Khruschev, and Castro on the Brink of Nuclear War.* New York: Vintage.
8. Draft Treaty on European Security Submitted by the Soviet Union at the Heads of Government Conference, Geneva (20 July 1955), https://www.cvce.eu/en/education/unit-content/-/unit/55c09dcc-a9f2-45e9-b240-eaef64452cae/c8516d5e-4bb4-448f-9f8e-ec0235487118/Resources#ce973fc0-f4d9-4bdc-b902-400ec6b31411_en&overlay, retrieved on 8 May 2024.
9. Fukuyama, F. (2007). *America at the Crossroads Democracy, Power, and the Neoconservative Legacy.* Paperback, https://yalebooks.yale.edu/book/9780300122534/america-at-the-crossroads/, retrieved on 20 May 2024.
10. Gaddis, J.L. (2021). *Războiul Rece. Înțelegerile, spionii, minciunile, adevărul.* Iași: Editura Polirom.
11. Garber, M., Walkowitz, R. (1995). *Secret Agents: The Rosenberg Case, McCarthyism and Fifties America*. New York: Routledge, https://books.google.ro/books, retrieved on 11 June 2024.
12. Gray, C. (2010). *Războiul, pacea și relațiile internaționale. O introducere în istoria strategică*. Iași: Editura Polirom.
13. Harris, W. (1965). *Chinese Nuclear Doctrine: The Decade prior to Weapons Development (1945-1955).* In *The China Quarterly* (21), http://www.jstor.org/stable/651319, retrieved on 15 April 2024.
14. Holloway, D. (1981). *Entering the Nuclear Arms Race: The Soviet Decision to Build the Atomic Bomb, 1939-45*. In *Social Studies of Science*, vol. 11.
15. Johnson, P. (2019). *O istorie a lumii moderne 1920-2000.* București: Editura Humanitas.
16. Kissinger, H. (2015). *Ordinea mondială. Reflecții asupra specificului națiunilor și a cursului istoriei.* București: Editura Rao Class.
17. Knight, A. (1993). *Beria: Stalin's First Lieutenant*. New Jersey: Princeton University Press.
18. Podvig, P. (ed.). (2004). *Russian strategic nuclear forces*. The Center for Arms Control, Energy and Environmental Studies at the Moscow Institute of Physics and Technology. The MIT Press. Cambridges, Massachusetts, https://books.google.ro/books, retrieved on 15 April 2021.
19. Sagan, C., Pollack, J.B., Ackerman, T.P., Toon, O.B.&Turco, R.P. (1983). *Nuclear Winter: Global Consequences of Multiple Nuclear Explosions*. In *Science*, 23 December 1983, vol. 222, no. 4630.

20. Sixsmith, M. (2021). *Rusia – un mileniu de istorie*. București: Editura Humanitas.
21. Tămaș, S. (1999). *Geopolitica*. București: Editura Institutului de Teorie Socială.
22. Time (1973). *Giving Them More Hell*, https://web.archive.org/web/20071012203926/http://www.time.com/time/magazine/article/0,9171,908217,00.html, retrieved on 12 May 2024.
23. Townshend, Ch. (ed.) (1997). *The Oxford Illustrated History of Modern War*. Oxford-New York: Oxford University Press.

HIGH ROYAL DECREE NO. 3663
THROUGH WHICH "ROMÂNIA MILITARĂ"
BECOMES THE OFFICIAL JOURNAL
OF THE GREAT GENERAL STAFF

"Art. I – The official journal named "România Militară" is founded at the Great General Staff, starting 1 January 1898, in which all officers within the Armed Forces will find military studies, which interest their training.

Through the agency of this journal, all oficers, belonging to all branches, who are in active duty, will be able to publish their personal papers and the ones that interest the Armed Forces".

Carol – King of Romania
Issued in Bucureşti on 8 December 1897

Order *"Meritul Cultural"*
in the rank of *"Knight"*, F Category
– *"Promotion of Culture"*
(Presidential Decree no. 646
on 24.08.2004)

Order *"Meritul Cultural"*
in the rank of *"Comandor"*, F Category
– *"Promotion of Culture"*
(Presidential Decree no. 483
on 10.05.2023)

Order *"Meritul Cultural"*
in the rank of *"Officer"*, F Category
– *"Promotion of Culture"*
(Presidential Decree no. 483
on 30.06.2014)

gmr.mapn.ro
facebook.com/gmr.mapn.ro