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

STRATEGIC IMPACT

No. 3-4 [84-85]/2022

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

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

CONTACT ADDRESS

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

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

CONTENTS

SCIENTIFIC EVENT

EDITOR'S NOTE

This Strategic Impact issue comprises volumes 84 and 85 for the year 2022, and is made up of six articles, followed by the Scientific Event section, where we share aspects of the topics addressed at the Scientific Seminar, held on October 28th, and the Workshop on December 14th.

Thereby, the first article in the ***Security and Military Strategy*** heading is written by our colleague, Colonel (Ret.) Researcher Crăișor-Constantin Ioniță, PhD, who continues his research on recent technological developments in the field of mosaic warfare, in the light of the competition for global and regional power.

In the second article, Captain Alexandru-Lucian Cucinschi, PhD Student, in co-authorship with Commander (Ret.) Professor Ion Chiorcea, PhD, analyses the extent to which obtaining inter-domain effects in multi-domain operation can be the necessary binder for the implementation of such an operation.

Next, Dragoș Ilinca, PhD, deals with the issue of linking cooperation in the field of armaments to the institutional framework of international organisations, such as the Western European Union, NATO and the European Union, in addition to the forms of cooperation between European states developed outside the EU or Allied framework.

In the ***Political-Military Topicality*** section, in a context where Russia is in the midst of a hybrid war to seize territory, Major Iulian-Constantin Mănăilescu, PhD Student, identifies Russia's current terrorist potential, which represents a real danger.

Under the heading ***Information Society***, Mrs. Cosmina-Andreea Neculcea, PhD Student, in co-authorship with Major General (Ret.) Professor Florian Răpan, PhD, presents a comparative study of the doctrinal projections specific to information operations (InfoOps), focusing on the US doctrines and combat manuals, as the originator of most of these documents − NATO doctrines and the local doctrines.

Mrs. Dana Ionela Drugă, PhD Student, signs an article whose aim is to raise awareness on the hostile actions of the Russian Federation in cyberspace, as well as the resilience of users to online messages.

The ***Scientific Event*** rubric briefly presents aspects of interest from the Scientific Seminar on the topic of Consolidated National Defence −Fundamental concept of operation for the Romanian Army 2021-2024, held online by CDSSS on October 28th. In the same section, details of the Workshop on the Impact of Climate Change on National Security, organised online on December 14th are also brought to the attention of our readers.

Moreover, we would like to point you to the updated ***Guide for Authors***, which is recommended for those who wish to disseminate their research results in the Strategic Impact journal.

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

Strategic Impact is an academic publication in the field of strategic defence and security studies journal that has been published since 2000 in Romanian, and since 2005 in English, in print and online. The articles are checked for plagiarism and scientifically evaluated (double blind peer review method). The thematic areas include political science, international relations, geopolitics, the political-military sphere, international organizations – with a focus on NATO and the EU information society, cyber security, intelligence studies and military history. Readers will find in the pages of the publication strategic-level analyses, syntheses and evaluations, views that explore the impact of national, regional and global dynamics. **Starting with issue no. 1/2023, the journal will be published exclusively in English**. The decision was taken to support authors in order to avoid duplication of effort and hopefully this will prove to be beneficial.

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

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

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

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

DOI: 10.53477/1842-9904-22-13

MULTI-DOMAIN OPERATIONS VERSUS "MOSAIC" WARFARE: THE LATEST TECHNOLOGICAL DEVELOPMENTS TO OPERATIONALISE THESE CONCEPTS

Crăișor-Constantin IONIȚĂ, PhD*

The fierce struggle for international (High Tech) market cornering and dominance is constantly taking place in the global Competition Continuum. The dominance of the technological market fits perfectly into the broad political-military disputes regarding the change of the current world order, in which competition between the great powers is becoming increasingly acute.

While MDO has grown in popularity among the military after including two new operational domains − space and cyberspace −, "mosaic" warfare is viewed more condescendingly by defence researchers, being explained much more technically, as an art of assembling small pieces (of coloured glass, stone, sandstone or other materials), hence its name.

As a result, the present paper aims to analyse the progress and continue to present the cutting-edge technological achievements of today according with those competition for global and regional power.

Keywords: *Multi-Domain Operations (MDO); the Mosaic Warfare; High-Tech; Competition Continuum; operational domain; Space; Cyberspace.*

**** Colonel (Ret.) Crăișor-Constantin IONIȚĂ, PhD is Researcher within the Centre for Defence and Security Strategic Studies of "Carol I" National Defence University, Bucharest, Romania. E-mail: ionita.constantin@unap.ro***

Introduction

The outbreak of the Russian − Ukrainian war has posed and continues to represent a very huge threat to Europe's security and the maintenance of the current international order. In addition to being considered the largest conventional military confrontation since World War II, Russian President Vladimir Putin's repeated threats to use nuclear weapons may turn it into World War III.

In addition, the fact that this war began and continues to unfold in the midst of the Coronavirus pandemic, with serious economic, financial and social consequences, as well as in the context of a global trend towards green energy and digitisation, there is an amplification of its consequences on regional and international security. Thus, we are already witnessing the emergence of international and regional crises such as the energy crisis, the humanitarian crisis (the increase in the number of migrants at the European level and the situation of social of the local population in conflict zones), the social crisis (decrease in the standard of living and the increase in the number of social movements against war, as well as the drastic measures taken by officials at European and national level), the food crisis (as a result of not distributing grains in time), as well as increasing the effects of climate change (such as drought, floods and hurricanes).

It can also be said that in this war, new types of weapons have been tested and continue to be tested by both the Russian and Allied forces, and that an unprecedented competition to dominate the international market development of emerging and disruptive technologies (EDTs) and the sale of their products has begun. A similar situation occurred during the Cold War, with the so-called "Star Wars", when Soviet-American competition to weaponise outer space led to the disintegration of the former Union of Soviet Socialist Republics (USSR) and the fall of communism. What sets it apart now is the larger number of participants (emerging states have been added), and the more diverse fields of technological development being at competition (artificial intelligence, robotics, unmanned vehicles, human performance enhancement/modification, nanotechnology, quantum physics, etc.).

The mere possession and use of new types of weapons, some of them very technologically advanced, is not the decisive factor for the rapid success of any of the parties involved in the conflict. This is the case of the Russian Air Force, which, although clearly superior to the Ukrainian one, did not even manage to achieve air superiority in certain strategic directions. The same can be said about equipping the Ukrainian Army with NATO-standard weapons systems − such as the Javelin, Milan or NLaws anti-tank missiles, the Stinger anti-aircraft missile or the 35 mm Ghepard self-propelled anti-aircraft gun (aka the "Cheetah"), the Harpoon anti-ship missile, the Himars artillery system, the M777 155mm towed howitzers, or self-propelled Panzerhaubitze (PzH) 2000, Zuzana or Krab, the M113 or Bushmaster

armored personnel carriers (APC) and the Bayraktar TB2 combat drones (UAVs) –, which only managed to provide it with tactical advantages.

Hence the need to develop operational concepts for the most efficient use of these advanced technologies in future armed conflicts. Currently, American military theorists have developed the concept of "Multi-Domain Operations (MDO)", which was immediately embraced by other Allied states and even by NATO, this being at the level of experimentation within the US Armed Forces. Apart of this endeavor, US researchers from the government's Defence Advanced Research Projects Agency (DARPA) have launched the concept of "the Mosaic Warfare" to outclass Russian Anti-Access and Area Denial (A2/AD) systems that prevent the US from intervening in regions controlled by Moscow and Beijing.

We have discussed and described these two operational concepts (MDO and Mosaic Warfare) in detail in articles previously published in the Strategic Impact journal, as well as in the specialised study entitled "Post-Industrial Society and Artificial Intelligence. Challenges and Opportunities from the Perspective of National Security and NATO Regarding the Development of the Multi-Domain Operation Concept", published in 2022 by the "Carol I" National Defence University Publishing House. As a result, this article analyses the latest conceptual approaches developed both at the level of the North Atlantic Alliance and of some member states and presents the new technological developments applicable to both concepts.

1. The Latest Conceptual Approaches of the Two Operational Concepts

The increase in existing threats and risks at European and Euro-Atlantic level and the emergence of new ones, caused by unprecedented technological developments in the civilian life but also at military level, have caused military strategists and defence researchers to rethink the way future armed conflicts are planned and conducted. The free access of state and non-state actors to advanced technological products, as well as the possibility to develop sophisticated weapon systems that restrict the freedom of action of Allied forces at a strategic level, or capabilities that act at the edge of legality, have amplified this necessity, accelerating the development of new operational concepts to make the use of new technologies more efficient and minimise those effects of adversary systems.

Within the Alliance, the term MDO has become extremely popular in recent years, starting with the US Army[1] and ending with the main Allied forces, even though there are still many member states and partners that have not defined the concept at the national level. In simple terms, the MDO represents the approach to future warfare (for the period 2025-2050) beyond the level represented by joint operations

[1] At the US Air Forces level the term used is *"Joint All-Domains Operations (JADO)"*, instead of *"Multi-Domain Operations (MDO)"*.

(Land, Air and Maritime) by incorporating two new recognised operational domains (Space and Cyberspace). Thus, MDO requires coordination of joint, interagency, and multinational military activities beyond campaign planning, where individual effects are combined at the boundary between the tactical and operational levels. And the specific degree of differentiation compared to joint operations is given both by the level of integration with the other instruments of power (in an authorised inter-agency approach) and by the level of expertise in the use of capabilities from all operational areas. (LTC Grest and LTC Heren 2019)

In essence, MDO is the synchronisation of the actions, forces and means of platforms (vehicles, satellites, ships, etc.), their Command and Control (C2) systems and all data sources to constitute a "complete picture of the operating battlespace" (see Figure no. 1) and to ensure the ability of warfighters in the Theater of Operations (ToO) and command staff to "rapidly make decisions that lead to action". (Tunnicliffe 2022)

Figure no. 1: The US approach for integrating all platforms into a large Command and Control network (Source: US DoD)

In future MDOs, the Artificial Intelligence (AI) and Machine Learning (ML) will play a critical role in helping staff personnel to manage large volumes of data (Big Data) and quickly decipher the most important information, and determine its operational relevance and then presenting informed options for shared decision-

making at all levels of C2. The ultimate goal is to overcome the adversary's strengths by presenting them with multiple operational and/or tactical dilemmas through the combined application of calibrated force posture, the employment of multi-domain formations, and the convergence of capabilities across domains, environments, and functions. As part of the implementation of this concept, all Services, but especially the Air Force and the Navy, are working on new technologies and capabilities through Research-Development-Innovation (CDI) programs, such as *"Project Overmatch"* and "*Advanced Battle Management System"*, respectively. Together, both force categories have developed more than a dozen collaborative technology projects, bringing together all operational domains to share and use intelligence, and assess and respond synergistically. Within the Ministry of Defence, the UK is developing the "Digital Backbone" transformation programme, which will enable information sharing and communication regardless of the hardware used. "We need to make sure that all the data we collect from every platform we have — whether it is satellite, aircraft, drone, ship or ground system – can be brought together to produce the most complete picture of what is happening". (Tunnicliffe 2022)

The North Atlantic Alliance has moved on to the definition of the MDO Concept and its development from September 2021. The development of the Allied MDO Concept was done in two phases–in June, NATO's definition and vision for Multi-Domain Operations were approved and, in September 2022, the Military Committee (MC) approved the original concept itself. Thus, according to the Allied approach, Multi-Domain Operations are defined as "the orchestration of military activities, in all domains and environments, synchronised with non-military activities, to enable the Alliance to produce convergent effects at a relevant speed". (The ACT Team 2022) In the Allied approach, effective implementation of the MDO can only be achieved through a cultural change within both the member states and the Alliance. This change involves moving from a traditional joint approach to one that is more broadly focused on all five operational domains, i.e. a fundamental shift of mindset towards Multi-Domain Operations.

At a conference jointly organised with the British Ministry of Defence in London a month later, some priorities for the development of this new concept were identified. The first priority is the development of the MDO as part of a broader integrated approach (diplomatic, informational, military and economic) at all member states level, complemented by partner education. Secondly, the question arose that the digital transformation of the organisation is understood by all Allies as a critical factor in developing the new concept by learning lessons from the Russian-Ukrainian conflict and continuing to develop capabilities, which they integrate into the "long-term approach to war". This long-term approach is carried out in accordance with the 20-year vision for the development of the Allies' military instrument of power, as part of the NATO Warfighting Capstone Concept (NWCC). Last but not least, it is intended to issue a development and implementation approach in phases, which

evolves towards achieving full interoperability of Allied forces and capabilities, with particular emphasis on the rapid development of those in the cyber and space domains. More specifically, "it is about ensuring that every part of defence can work seamlessly with other government departments, Allies and partners to achieve the desired outcome and to defend our NATO and nations." (Tunnicliffe 2022)

The most advanced allied state in the MDO is the US, which has already moved, at the level of the Army, to the concept operationalisation, by transforming it into a unified doctrine and testing "Multi-Domain Task Force (MDTF)" type of a force structure. After five years of development and experimentation, in June 2022, the United States Joint Doctrine on Multi-Domain Operations was approved, which has applicability in an anticipated operating battlespace for the year 2035 and an assessment of the security environment from 2025 to 2050. (Judson 2022) After testing the first MDTF in an operational-strategic exercise in the Pacific, the US Army developed a concept in March 2021 for operationalising five MDTFs to act in all phases of Competition Continuum (see Figure no. 2), including competition, crisis, and conflict. Two of these MDFTs will be deployed in the Indo-Pacific ToO (the first is already stationed at Lewis-McChord Joint Base in Washington D.C.), one in Europe and one in the Arctic. The fifth MDTF will be kept in reserve. As the document states, "each MDTF will be designed and adapted to operate at the necessary level to meet the needs of the supported Joint Force Commander. From the beginning, each MDTF will be assigned or tasked in support of a Strategic Commander (Combatant Commander), who will organise and train it according to the assigned missions." (Judson 2022) This new type of force structure will be coordinated by an MDTF All-Domain Operations Center (ADOC), which, once operationalised, will allow to ensure permanent contact with the adversary in all operational domains.

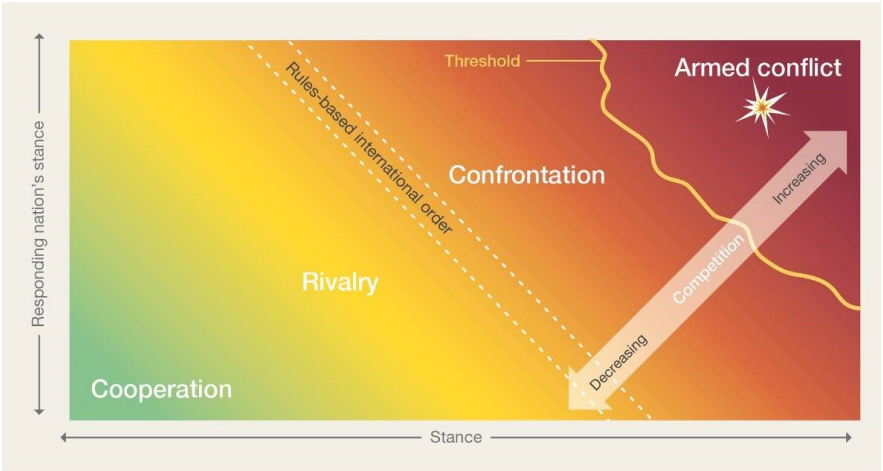


Figure no. 2: The specter of Competion Continuum
(Source: MCDC MD-MNU Project Report Nov 2022)

The second concept developed, this time by American defence researchers in the form of a strategy called "mosaic warfare", represents, in essence, an application of military art in the conduct of rapid military actions with measurable and tailored effects of a multi-domain lethal approach in future armed conflicts. Like the conglomerate from which it derives its name (mosaic), this new concept involves the use of a package of forces in which actions of individual combat platforms are fused in an artistic, innovative approach to the conduct of multiple attacks, in parallel and on a front wide, which ensures massing of fire and not forces to overwhelm the opponent. (Grayson 2018)

In the view of DARPA researchers, the mosaic warfare strategy incorporates the following areas of interest: technologies to operate in mosaic warfare, mosaic web services (EWS), experimentation with mosaic conceptual approaches, and the necessary fundamental strategic technologies and systems. Thus, the technologies that could operationalise this new strategy will need to provide solutions or automate functions such as: planning and organisation (e.g. software and automated decision tools to establish the core force structure or to increase the planning speed of commanders from theaters of operations), interoperability (a new global interoperability architecture applied to mission speed), and execution (for combining battle management decision support with machine autonomy). EWS involves the development of an advanced system-of-systems (SoS) incorporating new surveillance and search sensors and electronic warfare assets, particularly for the detection and capture portion of the kill chain and for achieving non-kinetic effects in offensive actions. Within the necessary fundamental strategic technologies and systems, it is foreseen to incorporate disruptive technologies that reduce the weight, volume, power or costs of some weapon systems, ensure their adaptability and quick refresh and ensure their advanced performance. (Strategic Technology Office 2018)

In the understanding of military researchers and technicians, "mosaic warfare" is a theory of war that involves forcing an adversary to fight with an unexpectedly large number of weapon systems and platforms of different classes, sizes and types, asymmetrically and variably arranged, where each acts distinctly like pieces of a mosaic, and which can create an overwhelming advantage compared to using systems and platforms similar to its own. (The Bae Systems Team 2021) The new strategy is also a multi-domain approach, in which the individual platforms of each operational domain (Air, Land, Maritime, Cyberspace, or Space), like pieces of a jigsaw puzzle, would together create a thorough picture of a large and overwhelming force, while making it more difficult for the adversary to identify an effective way to fight such a mixed and confusing force package.

To function effectively and bring a distinct strategic advantage to its user, the flexible nature of the new strategy requires flexibility in achieving communications

connectivity of all combat platforms and in planning their deployment and action in a coordinated, concentric and synergistic effort. Communications links and data sensors must be reliable and adaptable to interconnect state-of-the-art electronic warfare technologies (e.g. radio frequency/RF integrated analogue/digital mixed-signal electronics for high-capacity communications and electronic sensors precision systems that can increase situational awareness of own forces, improve weapons accuracy, and maintain communications flowing safely even in highly congested areas). In fact, this new approach represents the concept of using the most advanced technological products in the Decision-Centric Warfare[2].

At the same time, the asymmetric effects it propagates depend on the ability of the new strategy to introduce high-efficiency elements such as autonomous/remotely piloted aerial vehicles (UAVs), underwater (AUVs/UUVs) or ground-based vehicles (UGVs) and robots into the operating space, in an unexpected and amalgamated manner. These new means will increase the survivability of forces by considerably reducing the risks of human casualties.

As can be see, the two new concepts intertwine and represent a conceptual approach to the use the latest military technological developments in future armed conflicts. Thus, MDO is a pure military theory approach, in which the two new operational domains – Space and Cyberspace – are integrated within joint operations, as well as with the other instruments of power (see Figure no. 3).

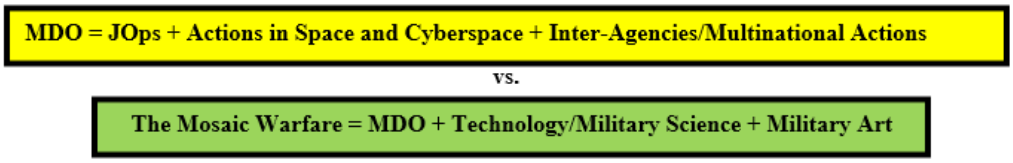


Figure no. 3: Multi-Domain Operations vs. the Mosaic Warfare

In turn, mosaic warfare strategy represents a multi-domain approach, but from the point of view of military art, in which the latest high-tech products are used in an innovative and unpredictable way to obtain asymmetric advantages over the adversary. Thus, the two new operational concepts bring attention to the development of multi-domain capabilities that include the highest technology products and that can act, interchangeably, in any operational domain or produce effects in domains other than the one for which they were established. At the same time, they also represent an innovative way of planning and conducting future armed conflicts, but the approach to each is different – MDO from the perspective of Military Theory and Mosaic Warfare from the perspective of Military Art.

[2] "The Decision-Centric Warfare" Concept replaces, in the US approach, the old "Network-Centric Warfare", used to increase the efficiency of the decision-making process through centralising it and it focuses on "the Mission Command" philosophy.

2. New Technological Developments within the Two Operational Concepts

At present, there is a real consensus among military specialists and policy makers that emerging and disruptive technologies (EDTs) have the potential to change the character of future wars. This desideratum is not a novelty because, throughout history, many newly introduced weapons have produced surprises or shocks at the strategic or operational level and influenced the outcome of wars. Such was the case with the use of fighter aircraft and chemical weapons (chlorine) in the First World War, the only means that brought an active approach to the static actions of all belligerents. Or the involvement of submarines and the tank-aircraft binomial by the German army to carry out the "Blitzkrieg", at the beginning of the Second World War. Not to mention the end of that war, when German V1 missiles, Japanese kamikaze tactics or the nuclear bombs launched by Americans at Hiroshima and Nagasaki were used. The Cold War began with the arms race for dual-launch ballistic missiles (nuclear and conventional) and continued with the competition to conquer outer space in the so-called "Star Wars".

But the biggest technological developments came after the end of the Cold War, when a new world order entered into force (the unipolar world) and the competition for world dominance reached its peak, leading to a possible change in the current international order (bi-polar or pluralism). Indeed, rapid advances in Artificial Intelligence, robotics, Big Data, quantum computing, and other emerging technologies may take future armed conflicts in new and unexpected directions. By developing new operational concepts for the use of advanced technological products, military organisations are expected to evolve, adapt and innovate to maintain a competitive advantage over state or non-state adversaries. In a future operating environment characterized by dimensional expansion, convergent domains and sensor proliferation, as well as an increase in weapon system range, speed, autonomy, lethality and compressed time horizons, the transformative impact of these technologies is likely to manifest itself across the entire spectrum of military engagement. That means, from major armed conflicts between great powers, to hybrid or hyper-war[3], to memetic warfare[4].

[3] The hyper-war was defined by General (ret.) John R. Allen and AI specialist Amir Husain in the science material *"On Hyper-War"* delivered at the US Naval Institute in July 2017 as *"a type of conflict in which human decision-making is almost entirely absent from the observation-orientation-decision (OODA) loop, being replaced by artificial intelligence. Consequently, the time associated with an OODA cycle will be reduced to almost instantaneous responses."* That is why it is also called *"the AI-fueled, machine-triggered conflict"*.

[4] NATO's Center of Excellence on STRATCOM in Riga, Latvia, defined memetic warfare as *"competition over narrative, ideas and social control in a social media battlefield; a subset of 'information operations' tailored to social media."* Information operations involve gathering and disseminating information to establish a competitive advantage over an adversary, and memes are like improvised explosive devices (IEDs) for information warfare – they are natural tools of an insurgency, very useful for throwing things in the air, but capable of sabotaging desired effects when used by the largest actor in an asymmetric conflict.

To implement the new operational concepts presented in the previous chapter, scientists and representatives of private defence companies investigated over 1,000 start-ups and emerging companies and established, according to Figure no. 4, the main trends in the transformation and use of advanced technological products to develop multi-domain capabilities, mapping the top 10 military technological innovations and their degree of impact in the near future. These technologies used in defence will bring changes to the military domain regarding connectivity (adversary detection and location, communication and conduct of direct operations), lethality (innovations in missiles and other attack platforms), autonomy (use of AI and robots to execute decisions with zero or minimal human involvement) and sustainability (strengthening the defence industry by adding 3D printing technologies and electrification) (The StartUs Team 2022).

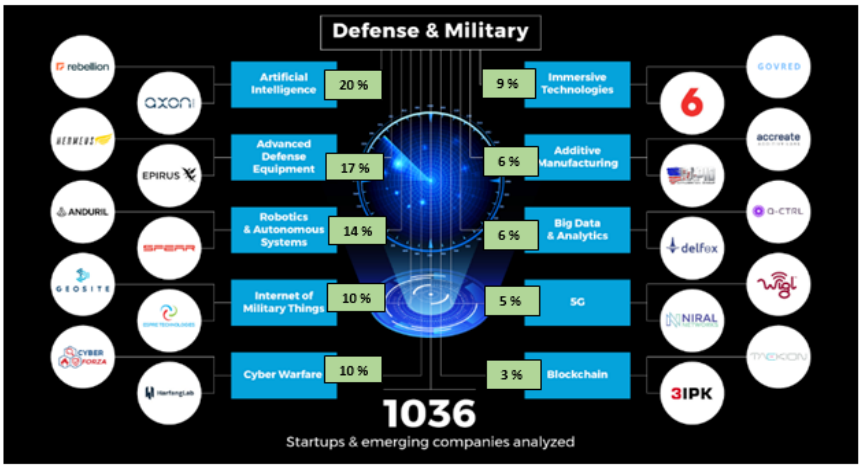


Figure no. 4: Top 10 of future trends in technological developments and their impact in the military field
(Source: Copyright@2021 StratUs Insights)

Topping these trends is Artificial Intelligence (AI). The implementation of the main AI products such as "digital twins" and "machine learning" in the military field will lead to improved algorithms and software for intelligence, surveillance and reconnaissance (ISR) missions. Computer vision will enable equipment safety management and provide a degree of empowerment for autonomous systems, thereby reducing military casualties (see Figure no. 5). But it should also not be forgotten that when AI can beat us at any kind of game, with the ease with which we beat chimpanzees today, the consequences can be catastrophic. This conclusion was reached at the same time by researchers from Google DeepMindo and the University of Oxford, stating that if advanced AI is left autonomously to use its own methods to achieve the set goals, allowing it to create their own tests and hypotheses, then

"an existential catastrophe is not only possible but probable." And AI software could intervene in providing information about the objective, with major consequences for the conduct of the attack phase (Mazilu 2022).

Figure no. 5: The possible Artificial Intelligence supremacy
(Source: https://Playtech.ro/2022)

Moreover, former Chinese Vice Minister of Foreign Affairs, Ms. Fu Ying, stated, in a scientific paper at Tsinghua University in December 2020, that "AI has limitations, including the inability to interpret intuition, emotion , responsibility and value. In the process of human-machine collaboration, the shortcomings of the machine could lead to the escalation of international crises." (Ying and Allen 2020) And her claim was reinforced by Chinese military analysts who argued that unmanned combat systems could encourage major military powers to use force, further dehumanise the enemy, and make the act of killing a simple game, which produces great collateral damage. Even a highly intelligent system would have difficulty discerning intentions on the battlefield when dealing with enemies who have been wounded or disarmed or who are using civilians as human shields. (Moriyasu and Fang 2021) As a result, leaving such decisions to machines can seriously undermine the distinction between civilians and combatants in international humanitarian law, as well as the rule that soldiers who have laid down their arms will not be subject to attack.

Despite all these inconveniences, China launched the world's first artificial intelligence-piloted drone carrier named "Zhu Hai Yun" in May 2022, which can transport 50 drones and unmanned aquatic and underwater systems on board (see Figure no. 6). Expected to enter service at the end of 2022, this unmanned vessel is 88 m long, 14 m wide and 6 m high, capable of developing a speed of 32 km/h and

is piloted by the AI "Intelligent Mobile Ocean Stereo Observing System", developed by the Southern Marine Science and Engineering Guangdong Laboratory. (Shoaib 2022)

Figure no. 6: China lauches the "Zhu Hai Yun" drone carrier
(Source: @venkatesh_Ragu)

The next place is occupied by the development of more sophisticated and technologically advanced defence equipment to deal with all types of threats and risks. Within this trend, innovations range from hypersonic flights to directed-energy weapon systems, including the advanced research in biotechnology and nanotechnology. Thus, in the field of hypersonic weapons[5], the competition is between Russia, China and the USA. As the deputy head of the US' Joint Chiefs of Staff, General John E. Hyten, stated in an interview with the Washington Post in February 2022, hypersonic missiles "...are the threats the future. This is not only because they can fly so fast, but also because their trajectory is so unpredictable. When tracking a ballistic missile, US surveillance systems can predict immediately after launch where it will land. But a hypersonic, low-altitude cruise missile can zigzag, avoiding detection and targeting and presenting a strange, perhaps unstoppable, hazard." (Ignatius 2022)

[5] Hypersonic weapons are of two kinds: a) hypersonic cruise missiles (HCMs), which are powered by high-performance air-propellans engines, known as scramjets (a hypersonic cruise missile is boosted by a hypersonic speed missile and then uses an air propellant engine to sustain that speed; b) hypersonic glide vehicles (HGVs), which comprise a manoeuvrable glide vehicle launched on a ballistic missile or booster rocket (an HGV is propelled by a high-altitude rocket and then glides towards its target, maneuvering along the way). Both types of weapons are notionally pre-programmed to fly to a specified target.

For now, a tangible advantage seems to be held by Russia, which has announced the existence of these hypersonic weapons systems since 2018 and has already tested and used in the Russian - Ukrainian war - the Avangard hypersonic glide vehicle (a 2-tonne strategic intercontinental ballistic missile, equipped with a UR-100NUTTH hypersonic vehicle flying at Mach 27 in low Earth orbit), as well as several types of hypersonic missiles, such as the 3M22 Zircon anti-ship/land target cruise missile (SS-N-33 in NATO, having a speed of Mach 9 and a range of 500-1,000 km, which can be launched from submarines or battleships) and the Kh-47M2 Kinzhal ('Dagger' in Russian lb. or RS) air-to-surface ballistic missile -AS-24 Killjoy in NATO, having a speed of Mach 12 and a range of 2,000 km, which can be launched from Tu-22M3 bombers and MIG-31K and Su-57 Felon interceptors). The Russian Air Force has had, since 1995 but upgraded in July 2018, a 53T6 hypersonic interceptor missile, called ABM-3 Gazelle by NATO, with a speed of Mach 17 and a range of 80-100 km, being kept in special silos . (The IISS Team 2022, 164-175)

For its part, China has joined the hypersonic arms race, testing on July 27 and August 13, 2022, its first Dong-Feng DF-ZF glider vehicle (designated by the US as WU-14, which has a speed of Mach 5 and can have a unpredictable trajectory in low Earth orbit up to a distance of 2,500 km, being built to be mounted on ground vehicles DF-17) on board of the Long Mach 2C space missile, as well as the anti-ship/anti-satellite ballistic missile DF- 21D (CSS-5 in NATO, having a speed of Mach 10 and a range of 1,770 km, which can be launched from submarines and DF-17 vehicles), developed jointly with Russia. (Makichuk 2022)

Recognising that it is lagging far behind, the US has accelerated testing of its supersonic weapons programs – the Air Force has an Air-Launched Rapid Response Weapon (ARRW) program in development for 2023, the Navy is developing two such "Conventional Prompt Strike" programs and "Hypersonic Air-Launched Offensive Anti-Surface Warfare" for 2028, the Army is working on the "Long-Range Hypersonic Weapon" programme and DARPA has the "Glide Breaker", "Tactical Boost Glide" and "MoHAWC" programmes in research and development. For its part, the US Missile Defence Agency (MDA) is considering the development of a system to destroy a hypersonic missile in the glide phase, which includes an interceptor as part of the Aegis system and the creation of a constellation of satellites (tracking hypersonic missiles on the flight path and guiding the interceptor to hit them) within the "Hypersonic and Ballistic Tracking Space Sensor (HBTSS)" programme. Thus, in mid-March 2022, it made the first flight of a hypersonic missile, called "Hypersonic Air-breathing Weapon Concept (HAWC)", produced by Lockheed Martin, with a speed of Mach 5 and being launched from a B-52 bomber. Four months later, the US Air Force tested two ARRW hypersonic missiles, also manufactured by Lockheed Martin, having a speed of Mach 6 and also being launched from aboard a B-52H, and DARPA carried out the first test of its hypersonic weapon

"Operational Fires". Furthermore, the US, UK and Australia announced on 6 April 2022 that they will collaborate under the newly created AUKUS Security Alliance (launched in September 2021) to jointly develop new types of hypersonic missiles to counterbalance de-escalation against China and Russia, through the hypersonic project "Southern Cross Integrated Flight Research Experiment". (Hamlin 2022)

As far as directed energy weapons systems[6] based on lasers are concerned, it can be said that there are only few countries in the world that have achieved some conclusive results in this field. This is because atmospheric thermal refraction still represents a difficult problem to solve. There is also the effect of permanent blindness under certain conditions of use, and its use as a non-lethal incapacitating weapon has been banned by the Protocol on the Prohibition of Laser Weapons that can cause Blinding, entered into force on July 30, 1998 and to which up to 109 UN member states have acceded. Currently, the most advanced laser system is the High-Energy Laser (HEL), which allows detection and engagement of a wide range of targets depending on its power, including unmanned vehicles, missile threats, ISR systems, missiles, ships, artillery and grenade launchers. The system's modular, adaptable design provides significant reductions in size, weight and power consumption to suit air, land and maritime platforms. Recent developments in laser weapons include: English "Dragonfire" strike system, Israeli "Iron Beam" anti-aircraft laser system, US naval anti-drone systems "Technology Maturation Laser Weapon System Demonstrator (LWSD)" and "AN/SEQ-2 Laser Weapon System (LaWS)", US naval anti-ship system "High Energy Laser and Integrated Optical-dazzler and Surveillance (HELIOS)", the US anti-RAM system "High Energy Liquid Laser Area Defence System (HELLADS)", which can be mounted on aircraft or combat vehicles, the US "Boeing Laser Avenger" land-based anti-drone system, installed on the AN/TWQ-1 Avenger combat vehicle, or the Russian "Almaz HEL" land-based system. (Spender 2022)

The US is currently working on a high-powered, 100-kilowatt laser weapon system, called HEL TVD, to be tested in 2023. This system will be able to inter-react with the Athena and Aladin laser systems designed for the US Air Force and Navy. At the level of the Russian Federation, it has been decided to build a new generation of powerful laser weapons, called "Zadira", already tested in Ukraine for the destruction of drones. And China is in the process of experimenting with high-powered electromagnetic pulse (EMP) weapon systems for multiple point defence and kinetically selected effects.

The unprecedented developments to date in robotics and autonomous weapon systems, with their tendencies towards full autonomy and the ethical implications of artificial intelligence, have caused certain states and multinational companies to

[6] Directed energy (DE) weapons include high-energy lasers, high-power radio frequency or microwave devices, and active or neutral particle beam weapons. In turn, microwaves and lasers are part of the electromagnetic spectrum, which includes light energy and radio waves.

question the degree of permissiveness and responsibility given to these so-called "killer robots". Seen as having an increasingly important role in future armed conflicts, robots and autonomous weapons systems are being developed to replace their own forces in tense or dangerous areas, and the idea of keeping the human factor in the decision-making equation is supported by most programmes developed. The biggest problem to be solved, apart from ethics, is the short response time, which sometimes exceeds the human capacity to react. As a result, the US Department of Defence (DoD) has developed some principles to focus on the responsible use of operating autonomous weapons systems in armed conflict, in a way that maintains human judgment and accountability over the use of force and helps minimize the likelihood of losing control over its system of inadvertent employment, particularly against non-combatants. These principles are based on the understanding of system autonomy in the military context as specified in DoD Directive 3000.09[7].

Internationally, it is increasingly being said that we are witnessing a veritable race to develop increasingly powerful robots and autonomous weapons systems, including, in addition to the US, great powers such as Great Britain, the Russian Federation and China. They are leading the development and testing of mobile robots, unmanned aerial systems (UAS or drones), marine autonomous vehicles, counter-explosive ordnance countermeasures (C-EOD) robots, surveillance and situational awareness, and material handling, humanoid/skeleton robots, swarms of drones or unmanned ground vehicles. The international market in this field is expected to grow to $52.16 billion by 2027, with a CAGR of 12.8% between 2020 and 2027. (After 2021)

A conclusive example of the use of autonomous drone weapon systems is the war between Azerbaijan and Armenia in 2020, when it was found that about 40% of Armenian tanks and armored vehicles, as well as over 90% of artillery and missiles were destroyed by drones acquired by Baku from the Turks and Israelis. (Moriyasu and Fang 2021) The same can be said of the use of the Turkiyesh Bayraktar TB2 drone by the Ukrainians against Russian forces, which literally changes the fate of the war, adding greater strike accuracy to Ukraine's airborne capabilities.

However, it is safe to say that the US continues to maintain its leadership position in the development of advanced military robots. To compete in the future robotics and autonomous weapons systems market, the Pentagon invested, last year, about 379 million dollars and continues to invest in the development of high-tech robots such as: The robot bee "The Robobee", a tiny static energy research or non-lethal

[7] DoD Directive (DoDD) 3000.09 "Autonomy in Weapon Systems" implements, along with "DoD's Artificial Intelligence (AI) Principles", the DoD's formal policy directives on autonomous weapon systems developed in 2012. The Directive is also consistent and with the 11 guiding principles established in 2019, in the framework of the Meeting of the High Contracting Parties to the Convention on the prohibition or restrictions on the use of certain conventional weapons that can be considered to be excessively harmful or to have non-discriminatory effects.

attack flying robot developed by the Harvard Microbiotic Laboratory that is capable of hovering for a short time or diving and being recharged via an electrical cable; The "DOGO" operative dog, a lightweight anti-terrorist combat robot that accompanies the military in combat, made by General Robotics and equipped with eight vision cameras, two audio negotiation systems and armed with a Glock 26 mm pistol or non-lethal weapons; The autonomous naval firefighting robot "SAFFIR" autonomous robot for fighting fires on board, developed by students at Virginia Tech University, which is equipped with stereo infrared vision sensors and a rotating laser, and equipped with extreme mechanisms claw-like grippers. (The RoboticsCareer Team 2021)

For its part, China has not let itself down and presented in Guandong, at the Zuhai Air Show of November 2022, the world's largest drone, called "Wing Loong-3", capable of transporting two tonnes of UAVs. At the same time, it tested a ground-based drone launch vehicle to be presented at the same air show, which was able to simultaneously launch 18 suicidal combat drones and which is produced by China Ordnance Equipment Group (CORG) to launch a so-called "barrage of drones" (see Figure no. 7). The catapult launch system on this vehicle will improve the survivability of swarm drone systems, such as the ASN-301/JWS-01 anti-radiation drone (modeled after Israel's Harpi loitering ammunition), being similar to the American "SwitchBlade 600". Apparently, this new system resembles the drone attack sequence in the American movie "Angel Has Fallen" and is inspired by the US naval drone attack project called "LOCUST" that started in 2015. (Hambling 2020)

Figure nr. 7: The "Hummer" − type vehicle with 48 UAV launching tubes
(Source: https://youtu.be/QamGaDNczJw)

Turkiye as well wants to be among the leading states in the development of unmanned combat aircraft, through its company Baykar, which announced, on

20 November 2022 that it had completed testing of its invisible supersonic drone "Kizilelma" (see Figure no. 8). This new drone can be classified as a 6th generation fighter aircraft, thus surpassing 4th generation aircraft, such as F-15 and F-16 (US), Rafale (France), Gripen (Sweden), SU-35 (Russia) and Eurofighter (EU), but also 5th generation ones, such as F-35 (US), SU-57 (Russia) and J-20 (China). Having the engine manufactured in cooperation with the company Ivchenko-Progress from Ukraine, the drone can carry 1,500 kg of ammunition, can reach an altitude of 10,000 m, has a range of 926 km and can stay in the air for up to five hours. These characteristics allow it to perform both air-to-ground and air-to-air missions, just like the latest generation manned combat aircraft. (Gheja 2022)

Figure no. 8: The Bayraktar Kizilelma supersonic invisible drone
(Source: Twitter - Baykar / Aktual24.ro)

Also, in the other technological trends – IoT, 5G, Cyber Warfare, imersive technologies, aditive manufacturing, Big Data or blockchain – research, developments and acquisition efforts are constantly changing and evolving. While they represent amazing technologies, they still require human effort to understand and employ them in future armed conflicts. As a result, they require special education and a special degree of training to be able to use them efficiently in the future operating space and work effectively in "man-machine" teams.

Conclusions

It is very true that the current competition between the great powers to acquire and deploy cutting-edge technologies has the effect of resuming the arms race and is

very similar to the Cold War-era's wining the space supremacy through the so-called "Star Wars". Now, when the world is facing numerous economic-financial, socio-humanitarian, energy and food crises, billions of euros/dollars are being spent to invest in state-of-the-art technological products to be used in future armed conflicts.

Using the latest and most advanced developments in military science and technology will create amazing and unique opportunities for the winner of the global technology competition to develop military capabilities that are difficult to counter. How to use these advanced technology capabilities will be conceptualised by new operational concepts in various stages of development or implementation, such as "Multi-Domain Operations (MDO)" or Mosaic Warfare. If MDO can be described as a synchronisation of the actions of platforms, forces and assets, their command and control systems and all data sources to constitute a complete picture of the operating battlespace and to ensure the ability to make rapid decisions that leading to action in a future operational space, mosaic warfare represents an application of Military Art in the conduct of rapid military actions, with measurable effects and adapted to a lethal multi-domain approach in future armed conflicts. Thus, both concepts aim at how to use advanced technological products in a future armed conflict, in a multi-domain, inter-agency and multinational approach. The main difference between the two operational concepts is the development framework of each − MDO is developed by military thinkers through the lens of Military Theory, to which they have added products of the Military Science, while the mosaic warfare is designed by defence researchers, combining Military Art with Military Science.

In the last decade, discussions have been gaining momentum at European and international level on how to use advanced technological products, especially lethal autonomous weapon systems (LAWS), in an attempt to solve the ethical aspects and legal restrictions according to the International Humanitarian Law. The lack of a unanimously agreed definition of LAWS has made these discussions difficult. However, a consensus was reached in 2019 to maintain human responsibility for decision-making on the use of these weapons systems and force through their use. Discussions are currently ongoing regarding the type and degree of involvement of human intervention required to ensure compliance with the provisions of International Humanitarian Law and resolve ethical interference. Ultimately, it is hoped that a Convention on the use of LAWS in combat will be adopted at the UN, respecting legal, ethical and moral principles.

Also, the forces intended to participate in future conflicts will be reorganised and tailored differently to achieve the effectiveness and teamwork of the "man-machine" binomial in the multidimensional operating space. But replacing fighters or human-manned systems with robots and autonomous weapons systems, as well as removing commanders from the decision-making cycle by introducing AI/ML software, will challenge the core philosophy of human existence − "Dubito ergo

cogito. Cogito ergo sum". And this is because machines, however advanced, will not have a degree of doubt in making technological decisions, but will act quickly and directly, as they have been programmed.

In such a fierce international competition, states with less economic power, such as Romania, will not be able to keep up and will become mere spectators, having to place themselves on one side or the other of the great competitive powers. This is why, at the level of the Romanian Armed Forces, the process of equipping with advanced technological products and developing an operational concept such as MDO, which would bring us among the modern Allied armies and counteract the possible threats and risks brought by the degree technology of potential adversaries. Especially since, as Elon Musk stated in his latest prophecies in November 2022, all forms of transport, including planes and ships, will become fully electric and largely autonomous, and tunnels will play an important role in the future of transport by 2030 (such as the electric sleds and cars on electric skates). The American billionaire's intention ist o use his SpaceX company to take people to Mars, by 2025, to colonise the planet. The American space agency NASA has already announced that the most powerful rocket in the world, the Space Launch System (SLS), has taken off on November 15, 2022 for the Moon, resuming the "Artemis" programme to colonise the Earth's natural satellite after 50 years.

BIBLIOGRAPHY:

Demaitre, Eugene. 2021. "10 Ground Robots in Development and Testing for Military Applications." *Robotics 24/7*, 05 31. Accessed on 10.11.2022. https://www.robotics247.com/article/10_ground_robots_military_applications/slideshow

Gheja, Victor. 2022. "Îngrijorare la Moscova. Baykar a lansat drona supersonică invizibilă Bayraktar Kizilelma: „Testele s-au finalizat cu succes" ."*AK-24*, 11 20. Accessed on 11.21.2022. https://www.aktual24.ro/panica-la-moscova-baykar-a-lansat-drona-supersonica-invizibila-bayraktar-kizilelma-testele-s-au-finalizat-cu-succes-video/

Grayson, Tim, interview by DARPA's Strategic Technology Office. 2018. "Breakthrough Technology: Past/Present/Future." *DARPA Tiles Together a Vision of Mosaic Warfare*. DARPA. 04 18. https://www.darpa.mil/work-with-us/darpa-tiles-together-a-vision-of-mosiac-warfare

Hambling, David. 2020. "China Releases Video Of New Barrage Swarm Drone Launcher."*Forbes*, 10 14. Accessed on 11.14.2022. https://www.forbes.com/sites/davidhambling/2020/10/14/china-releases-video-of-new-barrage-swarm-drone-launcher/?sh=407c9fb02ad7

Hamlin, Justin. 2022. "US Reveals Successful Tests of Hypersonic Missiles." *Asia Financial*, 07 14. Accessed on 10.10.2022. https://www.asiafinancial.com/us-reveals-successful-tests-of-hypersonic-missiles

Ignatius, David. 2022. "America led in hypersonic technology. Then other countries sped past." *The Washington Post*, 02 03. Accessed on 10.10.2022. https://www.washingtonpost.com/opinions/2022/02/03/america-led-hypersonic-technology-then-other-countries-sped-past/

Judson, Jen. 2022. "Multidomain operations concept will become doctrine this summer." *Defense News*. Accessed on 10. 06.2022. https://www.defensenews.com/land/2022/03/23/multidomain-operations-concept-will-become-doctrine-this-summer/

LTC Grest, Heiner, and Henry LTC Heren. 2019. "What is a Multi-Domain Operation?" Edited by JAPCC. Joint Air Power Competence Centre. Accessed 10 05, 2022. https://www.japcc.org/essays/what-is-a-multi-domain-operation/.

Makichuk, Dave. 2022. "China's Hypersonic Missiles Advantage Has West Worried." *Asia Financial*, 08 03. Accessed on 10.10.2022. https://www.asiafinancial.com/chinas-hypersonic-missiles-advantage-has-west-worried

Mazilu, Oana. 2022. "Un om de știință de la Google avertizează că o catastrofă existențială a inteligenței artificiale „nu este doar posibilă, ci probabilă"." *Playtech*, 09 16. Accessed on 10.07.2022. https://playtech.ro/2022/un-om-de-stiinta-de-la-google-avertizeaza-ca-o-catastrofa-existentiala-a-inteligentei-artificiale-nu-e-doar-posibila-ci-probabila/

Moriyasu, Ken, and Alex Fang. 2021. "Killer robots need ethical rules, US and Chinese analysts agree." *Nikkei Asia*, 05 26. Accessed on 10. 11.2022. https://asia.nikkei.com/Politics/International-relations/Indo-Pacific/Killer-robots-need-ethical-rules-US-and-Chinese-analysts-agree

Shoaib, Alia. 2022. "China launched the world's first AI-operated 'mother ship,' an unmanned carrier capable of launching dozens of drones." *Insider*, 06 11. Accessed on 11.14.2022. https://www.businessinsider.com/china-launches-worlds-first-ai-unmanned-drone-aircraft-carrier-2022-6

Spender, Tom. 2022. "Russia's laser weapon claim derided as propaganda." *BBC News*, 05 19. Accessed on 10.10.2022. https://www.bbc.com/news/world-europe-61508922

Strategic Technology Office. 2018. *darpa.mil.* 10 21. Accessed on 10.06.2022. https://www.darpa.mil/about-us/offices/sto/more

The ACT Team. 2022. "Multi-Domain Operations: Enabling NATO to Out-pace and Out-think its Adversaries." *ACT.* Accessed on 10.06.2022. https://www.act.nato.int/articles/multi-domain-operations-out-pacing-and-out-thinking-nato-adversaries

The Bae Systems Team. 2021. *BAE SUSTEMS.* 09 08. Accessed on 10.06.2022. https://www.baesystems.com/en-us/definition/mosaic-warfare

The IISS Team. 2022. *The Military Balance 2022.* London: Routlege Taylor&Francis Group.

The RoboticsCareer Team. 2021. "These are 3 of the Most Advanced Military Robots of the Future." *RoboticsCareer.org*, 09 01. Accessed on 10.11.2022. https://www.roboticscareer.org/news-and-events/news/23031

The StartUs Team. 2022. *Top 10 Military Technology Trends & Innovations for 2022.* Research, Reserach Blog, StartUs Insights. Accessed on 10. 07.2022. https://www.startus-insights.com/innovators-guide/top-10-military-technology-trends-2022/

Tunnicliffe, Andrew. 2022. "Multi-domain operations in the future battlespace." *Army Technology.* Accessed on 10.05.2022. https://www.army-technology.com/analysis/multi-domain-operations-in-the-future-battlespace/

Ying, Fu, and John Allen. 2020. *Together, The U.S. And China Can Reduce The Risks From AI.* Joint Report, Center for International Security and Strategy, Tsinghua University, Noema Magazine. Accessed on 10.11.2022. https://www.noemamag.com/together-the-u-s-and-china-can-reduce-the-risks-from-ai/

DOI: 10.53477/1842-9904-22-14

ACHIEVING INTER-DOMAINS EFFECTS – CHALLENGE IMPOSED BY THE MULTI-DOMAIN OPERATION

Alexandru-Lucian CUCINSCHI*
Ion CHIORCEA, PhD**

The multi-domain operation, although still insufficiently developed from a theoretical and, above all, practical point of view, can summarize the paradigm shift produced at the strategic level, a change caused by the developments in the current security environment. However, although this type of operation includes new types of technologies developed mainly as a pragmatic need by the tactical level and aims to achieve coherent solutions to counter the A2AD (anti-access and interdiction) threat at the strategic level, the coordination of the aspects necessary to carry out such operations currently seem rather difficult to achieve by the operational level, which aims at innovatively combining the specific tactics of the services to achieve operational and strategic level objectives. We consider that what is currently lacking as a tool for planning and conducting military actions is how to achieve inter-domains effects. Thus, in this article we will analyze the extent to which obtaining inter-domains effects in multi-domain operations can represent the necessary binder to implement such an operation.

Keywords: *military art; multi-domain operation; inter-domain effects; military action.*

**** Commander (N) Instructor Alexandru-Lucian CUCINSCHI is a PhD Student at the "Carol I" National Defence University, Bucharest, Romania. E-mail: cucinschi.alexandru@gmail.com***
***** Captain (N)(Ret.) Ion CHIORCEA, PhD, is a Professor at the "Mircea cel Bătrân" Naval Academy, Constanța, Romania. E-mail: chiorcea44@yahoo.com***

Introduction

The implementation of the multi-domain operation entails many challenges, as they are not limited to the integration of two new domains (cyber and space) within a conventional joint operation, and are of a complexity that in many cases exceeds the synthesis capacity of the current tools used by the military for planning and conducting military actions.

Thus, although initially the idea of integrating the two domains by the services was envisaged, at the tactical level, as the examples show: US Land Forces - US Land Forces in multi-domain operations 2028 (TRADOC, 2018); UK Air Force, by reforming the air groups so that they are able to respond to multi-domain threats (RAF, 2018) – one senses even from the ad hoc approach, at the level of the force categories, the necessary breadth to carry out such operations.

In this respect, the multi-domain operation has subsequently been approached mainly at the strategic level and less at the operational level, considering, first of all, its scope (it must be able to encompass the space and cyber domains, which are not entirely under military control). In addition, if at the tactical level some tools can be intuited by which new tactics can be deduced through exercises and experimentation and at the strategic level the goal, means and ways of achieving the goal are mostly known, at the operational level it is still quite difficult to determine how the actions of the services can work together to achieve strategic level objectives within the multi-domain operation.

However, the ways of implementing the multi-domain operation at the strategic level – NATO Warfighting Capstone Concept (Tammen, 2021); Integrated Operating Concept (UKMOD, Integrated Operating Concept, 2021) – shed light on expectations at the operational level. These, combined with the elements developed by the services in terms of multi-domain operation, can help identify the implications for the operational level.

Thus, operational-level concepts, such as Joint All Domain Command and Control (JADC2), which involves connecting sensors from all services into a single network with the aim of shortening decision-making time (CRS, 2022), aim to solve an operational-level problem: joint force command and control.

Similarly, the NATO Warfighting Capstone Concept, previously mentioned as a reference document for the strategic level, outlines five imperative directions for the development of combat (Tammen, 2021) including inter-domain command, leading to a dilemma as to the level at which the multi-domain operation can be managed from a command and control (strategic or operational) point of view.

The question is whether JADC2 (which we consider an operational level concept), which actually details the inter-domain command stipulated in the NATO Warfighting Capstone Concept (strategic level), is sufficient to bring the necessary

functionality to the operational level in the current security environment. In other words, is streamlining force command and control enough to gain an operational advantage over the adversary?

Based on the study, from the historical perspective of both the joint operation and the elements known to date about the multi-domain operation, we appreciate that the streamlining of command and control, although necessary, is not sufficient to provide the necessary coherence for the operational level so that it can be able to manage complex situations in a dynamic difficult to anticipate.

Thus, the hypothesis that we propose to test in this paper is as follows: If tools can be identified to achieve inter-domain effects, can the multi-domain operation contribute to the fulfillment of strategic objectives under the conditions imposed by the current security environment?

In order to so, we will analyze the known elements about the multi-domain operation at the tactical and strategic-military levels, then we will identify the challenges that the current security environment imposes on the operative level, and attempt to identify whether in the current security context the achievement of inter-domains can represent a viable tool for planning and conducting military actions at the operational level.

1. The Peculiarities of the Multi-Domain Operation at Tactical Level

Although in many cases the tactical level has overtaken the higher levels of military art in the sense of pushing the limits of the forces available through the initiatives of commanders, greatly influencing the fate of a conflict, nevertheless, as the current conflict in Ukraine has demonstrated, war won by a decisive battle is no longer possible in the vast majority of cases (Freedman, 2019).

An example of this is the Blitzkrieg, which, in the first part of the Second World War, contributed greatly to the successes of the German Army (the invasion of Poland, Denmark, Norway, Holland (the Netherlands), Belgium and France). Thus, the German Army, benefiting from the lessons identified in the past (von Moltke was a proponent of delegating authority to commanders at different levels), successfully applied this type of concept, a relevant example being the actions undertaken by General Heinz Guderian during the invasion of France. The latter, although he had been warned not to advance before sufficient infantry divisions had been brought into the battlespace in support of the armoured ones, after heated discussions with his superiors, sensing that the French were in disarray, advanced, paralyzing the French defence (Beevor, 2015). “So what would be erroneously described as a blitzkrieg strategy was largely an on-the-spot improvisation” (Beevor, 2015).

Currently, this type of tactical actions can only be carried out in the face of a clearly inferior adversary, in terms of combat power, considering the fact that with

the end of the Cold War, the Armed Forces ceased to represent a factor of progress in the technological field and the civilian/private sector took over this position. Thus, not having the most advanced technologies at their disposal, the military instrument of power began to depend to a large extent both on the state's other instruments of power of and on the large companies that develop new technologies for commercial purposes, but whose military applicability cannot be ignored.

As a result, at the tactical level, we consider that by promoting the multi-domain operation, there is an incorporation of new technologies into the tactical framework specific to each service, with the aim of identifying new ways of action.

Thus, the fact that the **Naval Forces** have come to the conclusion that, for practical reasons (involving risks) some of their actions can be executed by unmanned platforms, which can operate in all three specific environments (surface, submarine and air), is an aspect from which multi-domain operation can benefit in countering A2AD.

Also, artificial intelligence, by processing data from different sources (large databases), has led to improved maritime situational awareness, a fact that can indicate practical solutions, at a tactical level, for addressing concrete situations in the maritime domain that higher hierarchical levels (operational and strategic) need to consider.

However, if the incorporation of new methods of conducting military actions at the tactical level can bring the actions of the Naval Forces up to date with the specific reality of the maritime domain, in order to fulfil operational and strategic objectives, we consider that this must be accompanied by the development of new capabilities which will contribute to the implementation of the multi-domain operation in its ensemble.

The US **Army**, by publishing TRADOC Pamphlet 525-3-1−The US Army in multi-domain operations 2028, deals with the issue of the multi-domain operation more from a strategic and operational perspective and less at the tactical level, with the threat (A2/AD implemented by Russia and China) as the basis for the development of this operation.

However, the role of technology, although presented in terms of the possibilities available to potential adversaries, is considered as an essential premise in the development of the multi-domain operation: the proliferation of precision-guided weaponry, integrated air defence systems, cyberspace-specific weaponry, and other technologies enable a large number of potential adversaries to challenge and pose a risk to US Armed Forces in all domains, including the electromagnetic spectrum and the information environment at the tactical, operational, and strategic levels (TRADOC, 2018).

For the **Air Force**, a number of weapons companies have moved to develop solutions for implementing new technologies, both within existing military equipment and as new weapon systems that can operate in the battlespace. It is worth noting

that this equipment is being developed in the sense dictated by the multi-domain operation, to operate in several domains and inter-domains.

Thus, the Leonardo company offers specific weapon systems for multi-domain operations in addition to combat aircraft and helicopters equipped with state-of-the-art equipment and sensors, unmanned aerial vehicles (Falco EVO UAV) that can carry out a wide range of missions on land as and at sea thanks to innovative sensors, complete information integration solutions with surveillance data and modular avionics capable of managing a wide range of sensors, with the aim of accelerating and optimizing the decision-making process. The same company also offers solutions in the field of electronic warfare, such as the SAGE system (can be installed on a wide range of airborne platforms), which analyzes the electromagnetic spectrum in the air, land and sea environments to identify emissions sources and implicitly targets (Leonardo, 2022).

Airbus provides the military with systems that can counter cyber-attacks (MTLID) for the protection of military networks and data; unmanned aerial platforms (Aliaca UAS); IT solutions such as the multi-domain combat cloud, a tool that facilitates, by achieving information superiority, the collaboration of manned and unmanned vehicles during combat, in all environments (Airbus, 2022).

From the mentioned, we believe it can be stated that the tactical level has begun to incorporate new technologies into the specific capabilities of each service, with the observation that this process has been accelerated precisely by the affirmation of the intention to develop a new type of operations by the Armed Forces and the broad outline of its defining elements through the publication of studies and doctrines in this regard.

We thus observe that the development of this new concept, although based on new technologies that can be implemented by the tactical level, is not limited to them and also implies a statement of intent that, as is only natural, comes from the strategic level.

2. Contribution of the Strategy to the Development of Multi-Domain Operation

The strategic level, defined by different approaches, is best represented by two components that must be separated, given the specificity of each: strategic-political and strategic-military.

The strategic-political level is the one that launches the declaration of intent, as is the case of the multi-domain operation today, and it is responsible for the highest spheres of addressing relations between the actors (state and non-state) that dispute their primacy in different fields, including the military (where the issue of conflicts is also addressed).

Although most geopolitical and geostrategic specialists believe that „geopolitical disputes and rivalries start from the idea that in the globalizing international environment, economic means, and not necessarily military ones, are those that guarantee control, such as: access to stock market values from abroad; private direct investments; control of local currency reserves (either through the IMF and World Bank, or through multinational corporations in less developed countries); control of mineral resources, agriculture, manufacturing and other goods; and, last but not least, the organization and management of trade through foreign corporations" (Hlihor, 2005), we consider it our duty, as military personnel, to manage the ways in which the military tool can be used in support of economic means, but also as the main tool in case the economic means do not achieve the expected effect.

This declaration of intent is usually promoted through military strategy, although, as mentioned, the military instrument does not always play a central role, because it is the military that will ultimately guarantee the implementation of this strategy or, if this guarantee will not be considered effective, will move to forcing things in the direction established by the decision-makers at the strategic-political level.

Thus, we believe that a certain definition is relevant, from the perspective of identifying the defining element specific to military strategy: „military strategy consists of establishing military objectives and formulating strategic concepts for their fulfilment by using military resources to implement the concepts." (Potîrniche, 2020).

Figure no. 1: Military strategy components (Potîrniche, 2020)

Having presented, in Figure no. 1.1, the pillars on which the military strategy rests, we believe that it can be understood that setting the objectives does not require a special intellectual effort because, in most cases, it is quite easy to intuit what should be perform to reach a desired end state. Also, the issue of resources, although

complex and may involve considerable administrative efforts, depends more on organizational capacity and does not require a special intellectual effort.

On the other hand, the development of concepts, which in our opinion represent the essence of strategy, requires intense intellectual effort, and although it is difficult to quantify the outcome of this effort, we believe that the military's main responsibility is to understand how these concepts give a meaning to strategy and contribute to their continued development or improvement.

Currently the military strategy of NATO and most NATO member states and partners focuses on the design, development and application of the multi-domain operation concept. We are thus witnessing what is considered to be a process of military modernization based on this concept. This entails, firstly, an analysis of the future operating environment (where the threat is, in fact, the main element that is taken into account), then the identification of a concept (an idea that summarizes reality) and, finally, the development of new capabilities to be able to support the implementation of the concept, thus leading to countering the threat.

In the case of the multi-domain operation, A2AD represents, as with previous concepts (starting with the air-sea battle – 2009) the military problem that the US military must solve. A2AD capabilities have been considered those that threaten the ability of US and allied forces to get into a position to fight (access denial) as well as to fight effectively once in that position (maneuver denial) (ASBO, 2013).

Regarding the clarity of explanation of the A2AD concept, we find the following definitions of A2AD to be illuminating:

– A2 - action aimed at slowing down the deployment of own forces in a theatre of operations or forcing them to operate at a distance from the area where they would have been indicated to position themselves (affects movement);

– AD - action aimed at preventing own forces from operating in an area of operations where an adversary is unable or unwilling to deny access (affects the maneuver) (ASBO, 2013).

We notice that A2 hinders advantageous positioning, which is one of the components of operational planning, along with tactics and logistics, while AD prevents effective tactics, which indicates that *there will be great difficulties in operational planning*, logistics being also in a position to encounter difficulties if not addressed in time.

In response to this threat, the US, which has currently presented the most programmatic documents regarding the multi-domain operation, proposes a comprehensive approach of this type of concept, placing it at the strategic level, with implications for the operational level, while at the tactical level there is only the issue of multi-domain formations.

This is indicated by the division of the operation into phases: Competition, Penetration, Disintegration, Exploitation and Competition on favourable terms

(TRADOC, 2018). Analyzing, in the reference document mentioned, the aspects that make up these phases, we observe the extent necessary to command and control such an operation, an aspect that, in our opinion, cannot be managed by a level lower than the military-strategic level.

However, the military-strategic level cannot manage the correlation of tactics specific to each service, to which the cyber and space domains are currently added. This is the prerogative of the operational level, which, as von Moltke described it, as the level at which the military must not expect any political interference, must be able to achieve synergy (in the case of joint operation) and, more recently, convergence (in the case of multi-domain operation).

3. Multi-Domain Operation at Operative Level – Inter-Domain Effects

It is the operational level that must ultimately integrate, in a coherent way and adapted to the current threat, the tactics specific to the categories of forces, to which positioning and logistics are added. Operational planning is primarily the achievement of strategic goals by large combat units through a combination of positioning, tactics, and logistics (Skinner, 1988).

However, in addition to the military-strategic level threat, there is a threat specifically created for the operational level. Thus, the A2AD component, which aims at separating the joint force in time, space and combat functions, made the classic joint operations no longer possible to conduct except in an uncontested environment. Thus, high-precision, long-range weapon systems protected by anti-aircraft systems (both in multiple layers) create great problems for the joint force, both on the offensive and the defensive, with support between the services difficult to achieve. This is also the reason why, in order to compensate for these vulnerabilities, the cyber environment (2016) and later the space environment (2019) were first recognized as operational domains from which an advantage can be ensured for forces fighting in conventional environments. Moreover, these two environments can generate capabilities that can fight in place of some of the capabilities specific to conventional environments. This is what we consider of inter-domain effects.

As a result, we believe that following the model of the two new domains, this process should also be implemented within the classical environments, in order to successfully counter the A2AD threat at the operational level.

In this regard, in a previous personal paper, I suggested the following definition for the multi-domain operation at the operational level: "The ability of a service to temporarily fight in the specific domain (environment) of another service in order to provide an operational advantage with the aim of regaining/winning the initiative in that environment/domain" (Cucinschi, 2021).

We believe that by applying these inter-domain effects, it is possible to counteract, in the first phase, the separation of forces in time, a separation which, due to the specific nature of each category of forces, is easily exploited by the adversary (Table no. 1).

Table no. 1. Characteristics of the ground, air, maritime, and enduring virtual weapons cycles (TRADOC, 2018)

Cycle type	Build-up time	Persistence when employed	Reset interval
Ground	Very long (months)	Long (days)	Long (days - weeks)
Air	Short (days)	Short (hours)	Short (hours - days)
Maritime	Medium (weeks)	Very long (months)	Very long (weeks)
Virtual weapons (cyber, space, electronic warfare)	Short (days)	Very short (seconds - minutes)	Very short (minutes - hours)

After this separation in time (if successful) one can move to full control of an environment, which can allow exploitation of success in that environment, thus reaching the separation of combat and space functions.

This is the main reason why we believe that obtaining inter-domain effects is vital for multi-domain operation. If the separation in time succeeds for the adversary, the main advantage of the multi-domain approach to the operation, represented by the multiple options of own forces that turn into multiple dilemmas for the adversary, is nullified, the multi-domain operation thus tending towards a classical joint operation without much chance of success.

In the same vein, the UK Ministry of Defence has attempted, by publishing Joint Concept Note 1/17 − Future Force Concept, to explore the new relationships that can be established between or along the domains (UKMOD, Joint Concept Note 1/17 - Future Force Concept, 2017).

Conclusions

We consider that, unlike JCN 1/17, where inter-domain integration is considered sufficient to combat multiple threats in a single environment, to impose coherence on the actions of own forces as a whole, as a joint force and, and to build the

capabilities appropriate to a certain type of threat, the issue to explore and develop the best practices in terms of controlling spaces that until recently were inaccessible to them.

Because only by producing a pre-planned, intentional effect (as a result of an action) in the domain/environment specific to another service or in one of the two new domains (cyber and space) it is possible to determine the proportion of capabilities required for each domain as well as to identify asymmetric employment possibilities (the multitude of possible combinations), we appreciate that the inter-domain effects should be exploited in the sense of identifying them in time as well as the possibilities for their innovative combination.

By exploring these inter-domain effects, it is possible to build capabilities appropriate to concrete situations in a given geographic space, thus leading to what we have highlighted in Figure no. 2, within the tactical level – multi-domain formations, units that are area-specific, taking into account both the physical environment and the opponent.

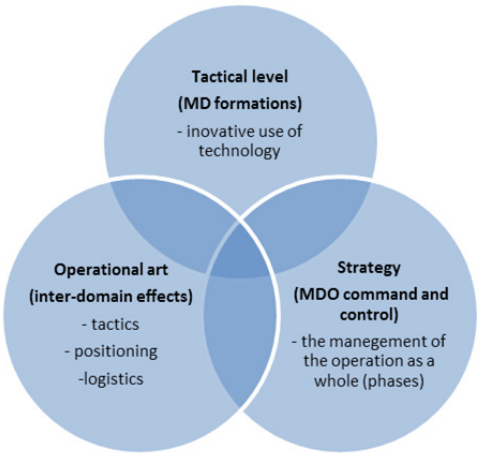


Figure no. 2: The implications of multi-domain operations to the military art components

In addition to the possible implications mentioned, we believe that it should also be highlighted that the current operations planning process (effects-based planning through the use of operational design) will have to undergo some changes, not only in the sense of integrating effects produced by the actions of one service in the specific domain of another service into the operational level design, but also in the sense of making the design elements more flexible, as they are currently increasingly rigid due to the computerization of decision-making, with computing machines leaving few aspects to the discretion of commanders.

BIBLIOGRAPHY:

Airbus. (2022). *Airbus Company*. Retrieved October 7, 2022, https://www.airbus.com/en/newsroom/stories/2022-06-airbus-brings-leading-edge-digital-capabilities-to-multi-domain-military.

ASBO. (2013). *Air-Sea Battle Office. Air-Sea Battle, Service Collaboration to Adrdress Anti-Access&Area Denial Challenges.*

Beevor, A. (2015). *Al Doilea Război Mondial.* București: Editura RAO.

CRS. (2022). *Congressional research Service.* Retrieved July 19, 2022, athttps://sgp.fas.org/crs/natsec/IF11493.pdf.

Cucinschi, A. (2021). *Operația întrunită și operația multi-domeniu – Delimitări conceptuale.* București: Biblioteca Universității Naționale de Apărare "Carol I".

Freedman, L. (2019). *Viitorul războiului, o istorie.* București: Editura Litera.

Hlihor, C. (2005). *Geopolitica și geostrategia în analiza relațiilor internaționale contemporane.* București: Editura Universității Naționale de Apărare "Carol I".

Leonardo. (2022). *FIDAE 2022: Leonardo's multi-domain technologies to meet every operational need.* Retrieved October 7, 2022, https://www.leonardo.com/en/news-and-stories-detail/-/detail/fidae-2022-leonardo.

Potîrniche, M. T. (2020). *Teorii și concepte strategice – Evaluarea prospectivă a stretegiei militare. Viitorul strategiei militare.* București: Editura Universității Naționale de Apărare "Carol I".

RAF. (2018). *Historic 11 Group reforms for multi-domain challenges.* Retrieved july 18, 2022, de pe https://www.raf.mod.uk/news/articles/historic-11-group-reforms-for-multi-domain-challenges/

Skinner, D. (1988). *Airland Battle Doctrine, Center for Naval Analysis.*

Tammen, J. W. (2021). *NATO's Warfighting Capstone Concept: anticipating the changing character of war.* Retrieved July 19, 2022, https://www.nato.int/docu/review/articles/2021/07/09/natos-warfighting-capstone-concept-anticipating-the-changing-character-of-war/index.html.

TRADOC. (2018). *TRADOC Pamphlet 525-3-1 – The US Army in multi-domain operations 2028.* Retrieved july 18, 2022, https://adminpubs.tradoc.army.mil/pamphlets/TP523-3-1.pdf.

UKMOD. (2017). *Joint Concept Note 1/17 – Future Force Concept.*

UKMOD. (2021). *Integrated Operating Concept.* Retrieved July 19, 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1014659/Integrated_Operating_Concept_2025.pdf.

DOI: 10.53477/1842-9904-22-15

HISTORICAL MILESTONES IN THE EVOLUTION OF EUROPEAN ARMAMENTS COOPERATION

Dragoș ILINCA, PhD*

European defence cooperation is one of the projects with a specific dynamism demonstrated in recent years through concrete initiatives with a certain multidisciplinary character. In this context, how European armaments cooperation supports the political objectives of sustaining an enhanced EU profile in the field of crisis management has been a priority. The practical reflection of this approach is related with a temporal perspective whose initial landmarks are set in the immediate post-Second World War. The development process evolved towards a European model of armaments cooperation based on two typologies. Firstly, they aim at associating armaments cooperation to the institutional framework of international organizations, as is the case with the Western European Union, NATO and the European Union. In addition, there are formulas of cooperation between European states developed outside the EU or NATO framework. Recent achievements indicate the feasibility of this solution, which also reflects the progress made in the overall process of developing the EU's profile and contribution as a relevant actor in the security context.

***Keywords**: EDC; CSDP; WEU; WEAG; WEAO; EDA; armaments; defence industry; OCCAR; LoI.*

Preliminary Remarks

Boosting cooperation in the field of armaments and, subsequently, the defence industry has been one of the lines of action constantly addressed in the context of

**** Dragoș ILINCA, PhD, is Research Coordinator within the Institute for Political Studies and Military History of Ministry of National Defence, Bucharest. Romania. E-mail: dilinca@yahoo.com***

the development of the security and defence dimension in the European context. Basically, one can speak of a generous historical perspective whose initial moments are found in the particular post-Second World War context, in which the Western European states engaged in identifying some cooperation formulas meant to ensure the security and defence of this geographical area.

Clearly, the focus of these concerns was to counter the Soviet threat by creating a system of alliances that would allow the creation of a common defence capability against any form of aggression. Equally, the recent experience of the Second World War has induced a specific dimension of Western European cooperation, particularly in relation to the possibility of German rearmament and, subsequently, how it could have contributed to the development of a new security and defence system in Western Europe.

In doing so, the defence industrial cooperation dimension has been one of the priorities. It can be seen as a precursor to institutional initiatives to coagulate European cooperation, as was the case with the European Coal and Steel Community (1951), the European Economic Community (1957) and the European Union. Obviously, we are talking about a relevant historical dimension of the maturing process of European armaments cooperation. The analysis of security and defence developments recorded in the decades following the end of the Second World War cannot exclude this dimension, given their importance for understanding contemporary realities. Interaction in this area has been an integral part of how European security has been addressed, the basic features of integrated policies at institutional level being defined during this period. Equally, the substance of cooperation has continued to revolve around elements and priorities developed successively in the post-war decades, as the European defence profile matured. There is thus a sustainable continuity between the different initiatives and concrete projects developed in the run-up to the creation of the European Union.

The specific nature of this dimension of cooperation made the developments recorded in the post-war period to be carried out both in connection with institutional developments recorded in the security context of the period and in intergovernmental formulas structured through the participation of Western European states in various configurations. From this perspective, the profile of European industrial cooperation can be regarded as a bivalent approach, including the formal-institutional component associated with the security and defence organizations created in Europe after the Second World War, respectively the cooperation formulas generated in the context of the development of the European Union, but not necessarily associated with this body. These coordinates include the assumption, since 2004, of the central role of the European Defence Agency (EDA) in setting capability priorities at European Union level, resulting in 2008 in the Capability Development Plan (CDP) to which all the Member States' efforts in the context of the Security and Defence Policy

will refer. In connection with this aspect, the role assumed at EDA level to facilitate cooperation between Member States in overcoming capability shortages is also placed. This aspect was addressed particularly in the context of the CSDP initiative launched under the name of the Coordinated Defence Review Process (CARD). Last but not least, the importance of the EDA is also validated from the perspective of functioning as an interface between the capability development process, research and technology, armaments and the defence industry, thus providing additional elements to support European defence cooperation.

In view of the complexity of the subject, the present study aims to provide a comprehensive overview of the path of European cooperation over the last half century. In this respect, structuring a historical perspective on how the security and defence objectives of European states have been reflected in the politically assumed priorities, is one of the main approaches. At the same time, the central thesis of the study considers that regardless of the institutional formulas developed between European states during this period, the European cooperation dimension in the field of armaments benefited from continuity, being able to be regarded as a red thread to which the national options were related. Even in the context of sinusoidal developments, the decades of cooperation before the advent of the European Union have provided the foundation that has allowed this area to be approached at a higher level. An important place is taken by the integrated approaches under the institutional auspices offered by the Western European Union (WEU) and, subsequently, the translation of its legacy to the European Union. The sources used mainly in underpinning this approach concern the decisions and procedural framework of WEU and NATO, with the deepening of the institutional approach to armaments cooperation.

Thus, the study provides additional elements of analysis for an issue that is dealt with, almost exclusively, only in the light of developments since the adoption of the Treaty of Lisbon. This approach generates a relative discontinuity in the understanding of the rationale behind armaments cooperation and, in particular, of the reasons that motivated the focus at European level. The study also provides the benchmarks in terms of the reasons that generated alternative formulas for cooperation between Member States. Thus, the study can also be regarded as a way of completing the existing bibliographical inventory in the field of European security and defence by offering another perspective on how the security and defence dimension has emerged at the level of the European Union. The thesis of continuity is also addressed from a transatlantic perspective, by looking in more depth at the issues of cooperation between the WEU and NATO, which has been the cornerstone in defining the EU's role in the field of security and defence.

In relation to continuity issues, the thesis on the priority given by Member States to the development of an integrated formula for governing armaments cooperation

is also placed. The constant approach to this subject has been carried out in close connection with the project of creating a Specialised Agency, being one of the first elements associated with an EU role in the field of defence that will be included in the Constitutive Treaty of the European Union. Thus, the study provides additional elements on how to formalize the aspects of cooperation in the field of armaments. In addition to assessing the major trends of evolution in these dimensions, the study also provides detailed elements on the different initiatives developed under the auspices of the WEU and NATO, thus contributing to strengthening the line of argument on continuity with the processes developed at EU level, by seizing the opportunities of the Lisbon Treaty.

1. Institutional Approaches

As is known, the first defence organization to emerge in post-war Europe was structured on the basis of the provisions of the Treaty of Brussels, signed on March 17, 1948, by France, Belgium, the Netherlands, Luxembourg and Great Britain. The main rationale for this approach was to initiate a format for cooperation in a wide range of areas between the former allied states in the Second World War, based on the Treaty of Dunkirk, signed by France and Great Britain. (Treaty of Economic, Social and Cultural Collaboration and Collective Self-Defence 1948). Under these auspices, the Western Union was established, with a structure dedicated to the field of defence, known as the Western Union Defence Organization (WUDO). It would operate until 1951 when its functions would be integrated into NATO. In its short existence, the issue of European defence industrial cooperation has not been addressed distinctly and at a higher level of depth, the priority of this organization being the creation of a defence capability against the Soviet threat. Concurrently with the development of the Western Union and the WUDO, the Organization for European Economic Cooperation was created on April 16, 1948, bringing together a much larger number[1] of Western European states. The work of this organization was closely linked to the elaboration of the Plan for the Recovery of Europe (1948-1951), which allowed the use of U.S. support through the Marshall Plan. This approach was firstly reflected in the post-war defence industry context, taken into an economically integrated perspective and with a direct link to the exploitation of natural resources and steel processing.

The issue of armaments and the possibility of developing a European defence, including their production, has been extensively addressed in the framework of the Treaty on the European Defence Community (EDC), signed on May 27,

[1] Austria, Belgium, Denmark, France, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Sweden, Switzerland, Turkey, Great Britain and West Germany (at that time represented by the European powers France, Great Britain, together with the USA).

1952, by France, the Federal Republic of Germany, Belgium, the Netherlands and Luxembourg. Basically, the implementation of the project for the development of a European army, on the coordinates agreed in the EDC Treaty, placed the European cooperation in the field of defence in connection with the industrial dimension of this profile through the development of the so-called joint endowment programmes. The failure to ratify the Treaty in the French Parliament (recorded after long debates on August 30, 1954) led to a temporary renunciation of this level of ambition. (Treaty Constituting the European defence Community 1952, 167)

In the context thus created, there was an amendment to the existing regulatory framework at the level of European cooperation, more precisely the Treaty of Brussels, which was to come into force in October 1954. As a result of this decision, a new defence organization came into being in Europe, under the name of the Western European Union (WEU), which practically took over the experience and functionalities fulfilled by the Western Union and the WUDO. Armaments was one of the new areas that will be included in the portfolio of this organization. It must be said that its approach was based, at least for the first decade, on controlling the production and types of armaments manufactured in Europe and, in particular, in Germany. It will become, together with Italy, a member of the WEU by amending the Brussels Treaty, assuming a number of obligations regarding the production and marketing of armaments. (Modified Brussels Treaty 1954) Under the auspices of the WEU, the issue of armaments has been addressed from several perspectives. Basically, the dimension of cooperation in the field of armaments was the main direction of action in which the WEU functioned, in the context in which, since 1960, the functions of sale in the economic, social and cultural fields have been taken over by the Council of Europe. Firstly, there was the Armaments Control Agency, created by the amendments to the Brussels Treaty, aimed at monitoring the production of military equipment and technology, as well as the existing stocks at Member State level. This entity will operate until 1985, when the WEU underwent an extensive reform process aimed at adapting to developments in the security environment in Europe and, at the same time, reflecting the state of play of the process of removing the effects of the Second World War.

In addition to the control and verification aspects, the dimension of cooperation between Member States to identify multinational solutions to facilitate national approaches in the field was addressed. This approach has been implemented through the Armaments Steering Committee which would operate until 1985, coordinating operational research activities, the evaluation of military equipment and technological experiments. Alongside this type of institutional approach, the development of European cooperation in the field of armaments recorded the emergence of the intergovernmental typology, with the creation, in 1976, of the Independent European Group (IEPG) with the participation of 13 states. The overall

aim of this approach was to promote a common European approach to armaments by: stimulating international cooperation in procurement; promoting standardization and interoperability; support for an industrial technological base for European and Allied defence; strengthening the European component in relation to the US and Canada.

Acting on the model of a consultation forum, the IEPG met annually at the level of defence ministers, while also including the format of the biannual meetings of national armaments directors. The structure of the IEPG also included a level of work, structured on three components: operational requirements and endowment programs; research and technologies; economic procedures and issues. (European Initiatives 1991, 24) The first ministerial meeting was held in The Hague in November 1984, during which priorities for cooperation between the participating states on armoured vehicles, medium-range surface-to-air missiles, transport aircraft were identified. Subsequently, the areas for cooperation were extended to include the research and technology dimension. At the same time, the work of the IEPG has also focused on the harmonisation of national procurement procedures, i.e. in terms of strengthening coordination between specialized structures in this field. The IEPG should also be seen from the perspective of contributing to the development of the conceptual inventory associated with European defence cooperation. Basically, the debates carried out within the IEPG introduce the concept of a "European armaments market" supported by an Action Plan on a Stepwise Development centered on the need to develop cross-border cooperation and which was to be a constant feature of the European debate from then on. (SIPRI 1992, 223-224) At the same time, the IEPG will also have a component dedicated to the cooperation with the defence industry that will be implemented through the European Defence Industries Group, an advisory structure that will provide expertise to the designated working groups. From the perspective of the contribution of IEPG to the development of concrete initiatives, the decision of the Ministers of Defence in June 1989 to launch a research and development initiative, known as EUCLID (European Cooperation for the Long-Term in Defence) is relevant, with the aim of developing 11 categories of capabilities in the European context (Common European Priorities), for each of which a state has been established as coordinator.

The forum approach to the armaments issue has included, in addition to the approaches mentioned, the emergence of other formats of dialogue and cooperation between Western European states. In parallel with the development of the EDC project, the issue of armaments in the European context has also seen other intergovernmental inspired approaches, as it is the case with the initiative of France, Italy, the Netherlands, Belgium and Luxembourg to create a formula for cooperation applicable to this domain. The approach resulted in the creation, through the Chiefs of Staff of the mentioned states, of FINABEL, an entity that was to identify measures to deepen coordination between European states in the field of land-based armaments.

The results recorded cannot necessarily be considered substantial consisting in the conclusion of agreements on technical specifications and operational concepts, their implementation being voluntary for member states.

In the context of the endeavors regarding the development of the Euro-Atlantic defence system, NATO's ways of strengthening the contribution of the European states generated particular formulas of cooperation. They have engaged a number of NATO European member states (Belgium, Denmark, Germany, Italy, Luxembourg, the Netherlands, Portugal, Spain, Turkey, Great Britain) in the EUROGROUP format, created on November 13, 1968, as a forum for interaction at the level of defence ministers. Under the auspices of this format, a working infrastructure has been developed targeting the areas identified as important for optimizing the European contribution to common defence.[2] Thus, seven working groups were organized in the fields of: communications in the theatre of operations (EUROCOM); logistics (EUROLOG); long-term planning (EUROLONGTERM); medical services (EUROMED); equipment collaboration (EURONAD); force structure (EUROSTRUCTURE), Joint training (EUROTRAINING). Note, from the perspective ofor the subject of this article, in particular the activity of EURONAD in which national representation was ensured at the level of the national directors for armaments. The main result of the efforts of this working group was the establishment of principles governing collaboration in the field of armaments, enhance standardization and interoperability. The inventory of principles will be approved at EUROGROUP level in 1972, including: the exchange of essential information between the participating states; assessment of the possibilities for cooperation; expanding cooperation in the procurement process; full standardization; maximum cooperation in logistic support; management and cost efficiency (Eurogroup 1976, 39-40).

2. WEU between Continuity and Failure

Significant changes in the institutional landscape associated with cooperation in the field of armaments have occurred against the background of WEU Member States's decision to develop a more visible profile (reactivation) of this organization. At the same time, the reason for this approach should be seen also from the perspective of strengthening the European contribution in the context of NATO, the Western European Union being perceived in the late 1980s as one of the important vectors in this direction. Thus, the WEU Council declaration of October 27, 1984, expressed

[2] Signed on April 3, 1948 by U.S. President Harry Truman (Economic Recovery Act). It will be known as the Marshall Plan, after the secretary of state, George Marshall, who was instrumental in its development.
Under the auspices of Eurogroup was adopted (1970) a European Defense Improvement Plan (EDIP) worth $ 1 billion that will run for a period of 5 years.

the determination of the Member States to develop the profile of that organization, including from the perspective of initiating a process of internal reorganization. The coming years will see major changes in the strategic framework within which the WEU revitalisation process will take place. Firstly, it is about implementing the convergence of views at the level of the Member States of the European Economic Community (EEC), aimed at moving to a higher level of cooperation through the creation of the European Union. Thus, with the entry into force of the Single European Act (1987), new areas of applicability of European cooperation under the aegis of the EEC were introduced, simultaneously with the introduction of European Political Cooperation, an instrument that will significantly contribute to the development of a new political-economic formula at European level. (Single European Act 1986, 7)

The WEU's place in this development would be clarified in the context of the Maastricht Treaty (signed on February 7, 1992, and entered into force on November 1, 1993) by which the European Union was created. From the perspective of the objective advanced by the Treaty in terms of "the implementation of a Common Defence Security Policy that over time can lead to a common defence" (Maastricht Treaty 1993, I,B), the WEU became an integral part of the European construction process, being the enabling structure empowered to implement EU decisions in the field of defence. On this note, the Declaration adopted by the WEU Member States on assuming the role of a component of the European Union in the field of defence as well as developing the cooperative relationship with the EU and NATO will be annexed to the text of the Treaty. Also, one of the points of the Declaration endorsed the development of cooperation in the field of armaments with the aim of creating a European Armaments Agency (Maastricht Treaty 1993, Declaration on Western Union). The achievement of this objective will strengthen the WEU's profile in terms of armaments cooperation, making it one of the main institutional benchmarks associated with this dimension.

Against this background, in December 1992, a decision was adopted to set up a specialized structure at WEU level in armaments issues. It will be named the Western European Armaments Group (WEAG), in the following years serving as an integrative platform for the various cooperation formulas developed in the European context in the field of armaments. On these coordinates, in December 1992, the Defence Ministers meeting in Bonn, in the format of the IEPG, decided to transfer the functions of this format to WEU. The main considerations of this decision were to ensure the continuity of the activities carried out under the auspices of the EDPS, as well as to better relate to the developments in the strategic framework for cooperation between the WEU and NATO. Last but not least, the transfer came to meet the political objective assumed by the Maastricht Treaty to develop the EU profile in the field of security and defence, all the more consolidated under the

objective of creating a specific agency for this sector (Duke 1994, 239-240). To an equal extent, the process of taking over three working groups developed under the auspices of EUROGROUP will be carried out, namely those on communications in the operational, logistic and long-term planning environment. At the same time, NATO will integrate the military equipment group into its own working formats with the participation of national armaments directors.

As a result of this process, the WEAG structure and its role in the coordination of armaments at the level of the participating states[3] was to be substantially strengthened. Responding to the trend of coagulation of the EU's defence role, WEAG's objectives were to: strengthen the technological and industrial defence base at European level; secure the necessary financial resources through a better harmonisation of operational requirements; improve cooperation in research and development; and open up national defence markets to international competition. In essence, the role of the WEAG was to serve as a platform for cooperation between Member States in order to identify and promote projects in the European context that had potential for industrial exploitation. The central role in coordinating activities within the WEAG was ensured by the defence ministers of the participating states, most often through the national armaments directors. In the institutional economy of the Western European Union, WEAG's role was to provide expertise in the field of armaments for the WEU Ministerial Council. From the perspective of the internal modus operandi, the WEAG structure targeted three components/panels. Panel I was responsible for harmonizing operational requirements and cooperation in the field of military equipment. The working modalities were to organise cooperation formats with the participation of the states concerned in working groups that regularly reported on the progress made. Depending on the complexity of the subject under consideration, there was the possibility of structuring within specialized working formulas (subgroups). The maximum level of cooperation under the aegis of Panel I included six thematic groups dedicated to air transport (strategic and tactical), missile development and portable launch capacity (WEAG: The Course To Be Followed 1995, 29). Panel II was dedicated to coordinating research and development activities in the field of defence (R&D) having as main fields of activity the development of priority areas for R&D at European level (forward-looking in terms of technological progress) and, subsequently, the coordination of research projects at their level.

Project funding was entirely the responsibility of the participating states, which contributed to limited progress in implementing practical solutions beyond the completion of feasibility studies. A distinct area of Panel II activity was the management of the EUCLID Program, inherited by the WEU following the process of taking over the responsibilities of the EIPG, which will be the platform for R&D

[3] 13 Member States participated, corresponding to the IEPG format. The only exceptions were Denmark (observer status), Norway and Turkey (associate members).

activities developed at WEAG level throughout its existence. The technological categories on which the program was structured represented the priority directions of action, being transposed into the priority areas. From this perspective, between 1995 and 1996, the work of Panel II was strengthened by the creation of an R&D Cell that will contribute to the implementation of the EUCLIDE program. The Third Panel was responsible for the prospective dimension over the development of strategic level projects aimed at creating a European defence equipment market. The main subjects[4] covered international competition, transparency of requirements, exchange of information on suppliers, common criteria for awarding contracts, etc. Progress during the existence of the WEAG has been limited due to the extension of the divergent political perspectives between WEU Member States on how to articulate such a project and in terms of its European character.

The implementation of the objective of the Maastricht Treaty to create a European Armaments Agency was also placed on similar lines. Discussions on this topic continued with intensity between 1994 and 1997, but without significant progress. In this context, developments relating to the coagulation of armaments cooperation formulas were further advanced by the decision of the bilateral Summit of France and Germany in Bonn (June 1994) aimed to create a Joint Armaments Agency. The project would evolve in the years to come with the inclusion of Great Britain and Italy in the Joint Armaments Cooperation Structure (JACS) which will come into being in January 1997. In parallel with the dynamism of the intergovernmental cooperation framework, efforts to implement the provisions of the Maastricht Treaty led to the emergence of the Western European Armaments Organisation (WEAO) as a subsidiary body of the WEU.

The main functions of the WEAO were to be agreed upon in terms of its compliance with the parameters set by the Maastricht Treaty. At the time, the option of using WEAO as a European armaments agency seemed to be the way forward. The functions agreed in 1997 by the WEAO Charter offered an extensive range of possibilities including: defence technology and research activities; endowment of defence equipment; development of studies in the field of defence; management of own goods and facilities. At the same time, the WEAO was an organization with legal personality, subsumed under that enjoyed by the WEU through the Paris Accords (European Armaments Cooperation 2003, 13). Along these lines, the WEU encompassed the two dimensions, research (through a Research Cell) and armaments, managed through the National Armaments Directors. The main message conveyed by the WEU Charter was that of an organizational development process in which the

[4] To a large extent, the benchmarks of the way in which the issue of the European arms market were on the coordinates advanced by the Vredling Report, drawn up in 1987 by a group of experts under the coordination of the former Dutch Minister of Defence Henk Vredeling (1973-1977). Its main theme was to reduce bureaucracy by deepening cooperation between European states and opening up markets.

transition to the next stage represented by the creation of the European Armaments Agency could have been carried out on the basis of a decision at ministerial level within the WEAG. In that case, WEAO would be involved in managing the different levels of the EUCLID program, taking responsibility for the award of contracts. Since 1999, a higher threshold has been established for awarding contracts (10% more) which would have included around 17 EUCLID contracts worth EUR 102 million. USD. (Luxembourg WEU Council 1999, 72)

The adoption of the Franco-British Declaration of St. Malo (December 1998) and, subsequently, the adoption of political decisions to launch the process of creating the EU's own capacity in the field of security and defence placed European cooperation within the WEU on a different course (From St.Malo to Nice 2001, 8-10). Thus, the new approach aimed at identifying those WEU functions that facilitated the implementation of the advanced vision in St.Malo regarding the EU's own capability for action in crisis management. The process of assessing which WEU instruments and facilities could be transferred to the EU was initiated by the decision of the WEU Ministerial Council in Luxembourg. In the context of this meeting, the defence ministers, meeting in the WEAG format, indicated their preference for connecting this format to future European armaments efforts.

The decision to adopt the first Global Defence Goal at EU level (Helsinki Headline Goal) following the European Council in December 1999 gave further impetus to the process of transferring WEU functions to the EU. Thus, the WEU Ministerial Council in Porto (15-16 May 2000) dealt extensively with this issue by adopting the decision to initiate a process of analysis on the long-term prospects of WEAG and WEAO in the light of developments at European level in the field of security and defence (From St.Malo to Nice 2001, 117). The next WEU Council meeting held in Marseilles (13 November 2000) was the end point of the WEU's existence, accepting the transfer[5] of the Agencies of the Institute for Security Studies and the Satellite Centre to the EU. It also advanced the deadline of July 1st, 2011, for the Western European Union to cease functioning, while maintaining the so-called residual functions[6] which would continue until the necessary framework for their takeover was created. They also included the issue of armaments, in particular the operation of WEAG and WEAO, whose integration also involved the takeover of ongoing programs.

Against the backdrop of the sharp dynamics of developments in the own security and defence dimension, the Treaty on the Constitution for Europe, adopted following

[5] They will be transformed into Agencies of the European Union by decision of the Nice European Council (December 2000).

[6] In addition to the role exercised by WEAG and WEAO, they concerned the WEU Parliamentary Assembly and the provisions of Article V of the Treaty of Brussels amended by the Paris Agreements. The latter concerned the mutual assistance clause between Member States.

the Convention of June-July 2003, strengthened the tendencies to takeover of the two entities. Thus, the objective of creating a European Agency for Military Capabilities, Research and Armaments was agreed. It was to identify the operational requirements and necessary implementing measures. It was also envisaged that the portfolio would also include the development of a defence technological and industrial base. It was also intended that the future agency would participate in the definition of capabilities and a European armaments policy, also play a role in supporting the EU Council in assessing the process of capability improvement (Treaty Establishing a Constitution for Europe 2003, Art.40). Although failed, the draft Constitution stated the parameters of the future structure, within which it became a formal reality of the option to take over the WEAG, the responsibilities of the projected agency reflecting the profile of the activities carried out by the WEU structure. The implementation of this objective had had a distinct route, in relation to the other components of the draft Constitution in the field of defence.

On February 24, 2003, the Franco-British Summit held in La Toquet marked the convergence of the two Member States towards the creation of a specialised Agency in the field of capability development and procurement. The support provided by France and the United Kingdom will be a strong stimulus for the practical implementation of this line of thinking, also reaffirmed by the first European Security Strategy adopted in December 2003. The continuity of references in the EU Treaties (Maastricht, Amsterdam, Nice) also provided the legal basis for the European Council's decision in May 2003 on the establishment, in the course of 2004, of an Intergovernmental Agency in the field of defence capability development, research, acquisition and armaments. Its tasks largely resumed the coordinates generated by the European Convention, while bringing additional elements regarding the coordination with the activities carried out by the European Commission on the security dimension.

The responsibility for implementing this objective and setting the parameters of the future agency has been taken over by the Italian Presidency of the EU Council, under the coordination of which a working group will be set up with the participation of the Member States. On 12 July 2004, the General Affairs and External Relations Council adopted the Joint Action on the establishment of the European Defence Agency (EDA) with the objectives of: the development of defence capabilities in the field of crisis management; promoting and strengthening European armaments cooperation; strengthening the European Technological and Industrial Base; the promotion, in cooperation with the Structures of the European Commission, of research procurement, including with a view to an enhanced role in the field of strategic defence technologies (COUNCIL JOINT ACTION 2004/551/CFSP 2004).

From an institutional perspective, the EDA was placed under the subordination of the High Representative and under the political authority of the Council. At the same time, it had legal personality, the financial aspects associated with its activity

being regulated by means of a three-year financial framework. The transfer of WEAG and WEAO to the European Defence Agency was completed between 2005 and 2006. The legacy of the two WEU entities encompassed around 300 projects (125 completed and the rest in various stages of development). The transfer process to EDA also included sizable projects representing, at least for the first years of operation, the essence of the portfolio of the new organization. Subsequently, EDA's role in the armaments dimension has developed significantly both on the conceptual dimension and by integrating this area into the overall context of capability development.

Conclusions

As it is clear from the previous pages, the development of European armaments cooperation and, subsequently, of the defence industry has undergone a sinuous development, marked by the political and military developments of the last half-century. However, it should be noted that this level of cooperation was one of the first areas addressed at the level of European defence cooperation, and it can be considered the forerunner of the political framework developed at European Union level associated with the Common Security and Defence Policy.

In this context, the creation of a specialized agency represented the red thread of the EU Treaties, an expression of the major political interest of the Member States in the development of this segment of cooperation, as well as of the convergence of opinions on the role of this entity in supporting the profile of the European Union in the field of crisis management. The operationalization of the Agency is one of the common points of the four Treaties adopted at EU level, not counting the Constitutional Treaty. It is also in this logic that references to the European Defence Agency in the Treaty of Lisbon are placed, all the more important at a time when this entity was created before the adoption of the last fundamental act for the functioning of the European Union.

On the substance, the different models addressed for establishing the responsibilities of such a structure have generally placed themselves in support of a coordination matrix that generates the framework for guiding European cooperation. The level of ambition associated with the role that such an organizational entity was to play in empowering the available funds was relatively constant throughout this period. The dominant option was to maintain the flexibility of the use of resources committed by the Member States. Thus, the creation of the relevant agency can be seen in the intergovernmental key governing European security and defence cooperation, where the EDA is intended to ensure the reflection of the entire set of options and positions of the Member States. Although not very visible in terms of the level of resources at its disposal, the added value of the European Defence Agency lies in the ability to project common perspectives on the priorities to which European

cooperation must respond and, last but not least, to allow for the identification of common solutions to remedy existing shortcomings and gaps.

Equally, one can also speak of a variable geometry of European armaments cooperation formulas that has incorporated both WEAG, WEAO and, at present, EDA-type formulas, as well as cooperation arrangements between European states. The coexistence of these models is one of the characteristics of armaments cooperation, and all the more important in the context of the defence industry. In this context, it is worth mentioning initiatives such as the Organisation for Joint Cooperation in the field of Armaments (OCCAR) formed in 1996 (Germany, France, Italy, Spain, Luxembourg, the Netherlands and the United Kingdom) or the Framework Agreement, signed in July 2000 (Germany, France, Italy, Spain, Sweden, the Netherlands and the United Kingdom) which are elements validating this trend. The existence of these two typologies of approach to the armaments issue, in connection with the industrial dimension, is the basic feature of European cooperation in this area, which will be maintained for the immediate future.

BIBLIOGRAPHY:

COUNCIL JOINT ACTION 2004/551/CFSP of 12 July 2004 on the establishment of the European Defence Agency.

EU Global Strategy – Shared Vision, Common Action: A Stronger Europe, June, 2016.

EU Security Strategy – A Secure Europe in A Better World, December, 2003

European Union – Cologne European Council, Presidency Conclusion, 3-4 June, 1999.

European Union Institue for Security Studies – *European Armaments Cooperation*, Chaillot Papers, nr.59, Paris, 2003.

EU Maastricht Treaty, Official Journal of the European Communities, Nr. C 191, 29.07.1992.

European Communities Commission - Single European Act, Bulletin of the European Communities Supplement 2/86, Luxembourg, 1986.

IEPG – Action Plan on a Stepwise Development of a European Armaments Market, IEPG document NAD/D-22. 23 septembrie 1988.

Independent European Programme Group. European Defence Industry Study Team – *Towards a Stronger Europe: A Report by an Independent Study Team Established by Defence Ministers of Nations of the Independent European Programme Group to Make Proposals to Improve the Competitiveness of Europe's Defence Equipment Industry*, 1987.

NATO – The Eurogroup, Bruxelles, 1976.

Simon Duke – The New European Security Disorder, Palgrave MacMillan, 1994

SIPRI – Restructuring of Arms Production in Western Europe, Oxford University Press, 1992.

Treaty of Alliance and Mutual Assistance, Dunkirk, March, 4, 1947.

Treaty constituting the European Defence Community, May, 27, 1952.

Treaty Establishing a Constitution for Europe, 2003.

United States General Accounting Office – *European Initiatives. Implications for US Defence Trade and Cooperation*, Washington DC, 1991.

Western Union – Treaty of Economic, Social and Cultural Collaboration and Collective Self-Defence, Bruxelles, 17 March 1948.

Western European Union – Brussels Treaty. As amended by the Protocol modifying and completing the Brussels Treaty, signed at Paris on October 23, 1954.

Western European Union – Ministerial Council, Luxembourg, 22-23 November 1999.

Western European Union Institute for Security Studies. *From St.Malo to Nice. European Defence: Core Documents*, Paris, 2001.

WEU Assembly – WEAG: the course to be followed, Paris, 1995.

DOI: 10.53477/1842-9904-22-16

RUSSIAN TERRORISM – A REAL DANGER TO EUROPEAN SECURITY

Iulian-Constantin MĂNĂILESCU*

Today, amid the imperial dream, in a context where Russia is in the midst of a territorial war (the one in Ukraine) carried out with hybrid means, coupled with a recent history of Russian terrorist attacks of several types, the question of an imminent danger to the security of the democratic European region may be raised. Thus, the analysis starts from the hypothesis that Europe is facing a new terrorist danger promoted by Russia, developed against the background of actions to destabilise the democratic order through hybrid warfare, with great risk to regional security.

In this regard, the purpose of the article is to identify Russia's terrorist potential at present. Its subsumed objectives are to analyse the three growing dangers that build Russia's terrorist potential. The first threat is the turbulent history of terrorism in this country. The second danger relates to the existence of a military group that has carried out several terrorist actions outside Russian territory, the Wagner group. The third danger is the activation of Islamist terrorism in Ukraine, by enlisting in the Russian army and training radicalized fighters from Muslim countries under Russian rule. The main research method is documentation. Studies, press articles and statistics on the subject were analysed, on the basis of which conclusions were drawn.

Keywords: *terrorism; security; hybrid warfare; Russian danger; Wagner.*

Introduction

Since the start of the war in Ukraine, the word "terrorism" has taken on new meanings, especially in the context in which four states (Poland, Lithuania, Latvia, Estonia) of the European Union have declared Russia to be a "terrorist regime". In

**** Iulian-Constantin MĂNĂILESCU is a PhD Student in the field of Public Order and National Security at the "Alexandru Ioan Cuza" Police Academy, Bucharest, Romania. Email: driulianmanailescu@yahoo.com***

November, the European Parliament, meeting in plenary session, declared Russia a "state sponsoring terrorism and using terrorist means" (HotNews.ro 2022). With regard to the United States of America, its position on considering Russia as a "terrorist state", formulated by NATO Ambassador Julianne Smith, is seen as "counterproductive, in the sense that it could slow down or obstruct our ability to send humanitarian assistance to Ukraine, or export grain from Ukraine" (Toader 2022). This article does not seek to explain what it means for a state to be declared 'terrorist'. The only point to be made on this issue is the conclusion resulting from the content of the article on "How international relations change the declaration of Russia as a "terrorist regime", published by *Europa Liberă* in early November, that there is no unitary position of the world's states on state terrorism. The analysis contained in the paper focuses on identifying the potential of this country to carry out globally recognized terrorist actions, such as bombings, chemical or biological attacks.

The terrorist potential of a state must be analysed in the context of its terrorist history. In the case of Russia, the country has, for many years now, engaged in various initiatives to undermine other societies in order to achieve the objectives of President Putin and his regime. Such actions include cyberattacks, meddling in elections and political processes using official propaganda tools such as Russia Today and Sputnik, complemented by more subtle disinformation programmes. At the same time, conventional and unconventional manifestations of armed intervention in the vicinity of Russia have taken place. All of these can be included in what is called "hybrid warfare" (Orenstein 2019). Also, the Russian authorities of the Putin regime have put into practice several acts of terrorism in several countries characterized by an open society (Great Britain and Germany). The assassinations or assassination attempts carried out by Kremlin agents (some of whom have even received various distinctions for these acts), in which they used radioactive elements, chemicals or firearms, are already notorious. For example, the European Court of Human Rights found the Kremlin responsible for the 2006 murder by radiation poisoning of Alexander Litvinenko, a former Russian intelligence official who defected to the West. The Kremlin has denied any involvement in Litvinenko's death, moreover, the two assassins, Lugovoi and Kovtun, appointed Russian agents by the ECHR, have suggested that the deserter may have poisoned himself (Newman 2021). Another case is that of Zelimkhan Khangoshvili, a Georgian Chechen, who was shot and killed on his way to a mosque in Berlin's small Kleiner Tiergarten Park. Khangoshvili had fought against Russian troops in Chechnya and, despite denying involvement in his death, Russia has long classified him as a "terrorist" (Holroyd 2021). The targets of these attacks were mainly opponents of the regime seeking support in the West (Filipov 2017). Such an action also took place in Ukraine in 2004, when Viktor Yushchenko, whose victory in the elections did not fit Moscow's plans, was poisoned with dioxin (Rupar 2014).

Russia's link with terrorism, totally different from that of democratic countries, is also reflected in its anti-terrorist legislation (Analysis 2010). It mainly targets the jihadist threat, but Putin uses it to regulate the persecution of any form of opposition to his regime. Externally, the Russian position is contrary to counterterrorist statements, for example, supporting Bashar al-Assad in his campaign against non-jihadist opposition groups (Rahman-Jones 2017) as he accepted the displacement of foreign terrorist fighters from countries of the Russian Federation, Chechnya and Dagestan, in Syria and other conflict zones where Islamist militants are active. This maneuver brought an advantage to Russia because it meant dislodging terrorists who would have posed a threat to it from its territories of interest (Borshchevskaya n.d.).

As will be demonstrated below, Russia's hybrid war against the Western world comprises a terrorist component. Moscow has so far shown that it is willing to use terrorism to achieve its interests, even though it has had policies to distract the West from its terrorist actions by promoting anti-jihadist actions. The war in Ukraine has brought the subject back to the attention of European authorities responsible for regional security. It is not necessary for the end of this war to limit these actions, since they are part of Russia's foreign instruments of warfare.

Hybrid warfare is a military strategy that combines conventional warfare, irregular warfare, cyber warfare, subversion, and blurs the formal distinction between war and peace. It is often characterised by the use of fictitious propaganda, espionage, ethnic mobilisation, linguistic or confessional minorities and terrorism.

1. History of Russian Terrorism

Terrorism has been present as a phenomenon in the Russian social and political for a long time. This is confirmed by the fact that as early as the 16th century, there have been legal provisions in Russia that address this issue. Most of them are related to the annihilation of any threat to the tsarist power. Terrorist events intensified during the 19th century and the phenomenon acquired certain distinct features: nationalist, revolutionary and highly reactionary (Laskowska n.d.).

To understand Russian terrorism, it is necessary to understand the history of terrorism in this country, and especially the way in which the power and population related to it. A first step in obtaining this agreement is to examine the events of the autumn of 1905, when Lenin forced the Bolshevik Party to take actions that sowed terror and which he called "guerrilla war". These actions of revolutionary terror were accepted by a large part of the population and became a mass phenomenon. The explanation is that "the revolutionary actions were a response to the tsarist actions against those who opposed the regime: death penalty, deprivation of liberty, exile to penal colonies, prohibition to establish residence in certain places, prohibition of the possession of specific offices or where specific activities were carried out,

expulsion of perpetrators from universities, their ban on entering or leaving the country" (Blackmore 2020).

After 1917, Russia experienced unique forms of politics and ideological terrorism: revolutionary (red) and counter-revolutionary (white) terrorism during the revolution and the civil war that followed; internal state terrorism during Stalin's political repression; international state terrorism during the period of domination by the Soviet authorities. These forms were not criminalised during their emergence and were not considered by society and the state as political terrorism until the collapse of the socialist system (Laskowska n.d.).

State terrorism in the Soviet period, especially during the Stalin era, was monstrous. To rule, the Soviet state established a unique system of administration of justice aimed at destroying political opponents. Millions of people have died or suffered repression for political reasons. According to W.W. Luneev, during that period about 40 million people were victims of repression (Getty 2002). Because of Stalin, society was terrorized with hideous, albeit effective methods, used to introduce and preserve totalitarianism, by creating a system whereby people were crushed at every attempt to oppose the regime. For a long time, the term terrorism was not used in Russia. After 1970, the government in Moscow named terrorist acts: 1973 – an explosion of a plane flying from Moscow to Chita; 1978 – a series of explosions in the Moscow metro; 1982 – hijacking of an aircraft flying to Turkey; 1983 – hijacking of a plane at Tbilisi airport and an assassination attempt on the life of the First Secretary and other leaders of the Communist Party (Laskowska n.d.).

With Perestroika, terrorist actions appeared in countries that wanted to gain independence from the USSR. After 1990, these actions intensified. The term terrorism begins to be used in a sense close to that of the democratic world. Among the countries where terrorist actions took place at that time were Azerbaijan, Armenia, Georgia, Tajikistan and Uzbekistan (Laskowska n.d.). After the collapse of the USSR, terrorism in Ukraine is primarily linked to Chechnya. In 1991, the Supreme Council of the Chechnya Republic was abolished and power would pass to the Chechen people. Such action led to a war and, implicitly, to the formation of terrorist-type groups, which operated both in Russia and abroad and which became increasingly active (C.Walters 2019).

The terrorist attacks that followed in response to the actions of the Russian government (especially the Russian army) involved hostage-taking (Budyoovsk – 1995, Pervomaiskoye – 1996), as well as other more violent actions and better organized attacks (attacks on the Dubrovka theatre in Moscow in 2002 and the school in Beslan in 2004) (C.Walters 2019).

In conclusion, Russian terrorism most often springs from political reasons, which reflect the difficult and complex situation of the Russian state.

2. Wagner Group – Terrorist Group

The Wagner Group has sparked controversy since the day of its establishment. A Russian paramilitary organization, the mercenary group carried out operations that the Russian Ministry of Defence silently approved, while maintaining plausible deniability. After years of denial and silence, the Kremlin has officially acknowledged the organization's existence, despite the fact that mercenaries are illegal under the Russian Constitution (McBride 2022).

The Wagner Group is currently led by Yevgeny Prigozhin, an important figure in the Kremlin. Prigozhin has cultivated a cult of personality through the organization's activities, openly attacking the Russian Ministry of Defence for battlefield losses in Ukraine and, more recently, opening a "Wagner Center" in St. Petersburg to help incubate start-ups with IT potential military applications (McBride 2022). Dmitry Utkin, a far-right GRU officer, is also at the head of the mercenary group. Wagner has sought to recruit far-right people not only from Russia, but also from among foreigners who can use the group's tactics in their home countries if necessary. For example, the Rusich Group, a subsidiary of the Wagner Group, openly recruits neo-Nazis, fascists and dughinists into its ranks (Dinu 2022).

The Wagner Group paramilitaries have taken part in military operations in Ukraine, Syria, North Africa and the Central African Republic, their operations being truly bloody, involving numerous massacres (Dinu 2022).

Wagner has earned the status of a shadowy organisation in Ukraine's Donbas region since 2014, when it took part in military operations at the behest of the GRU by arming pro-Russian militias. Wagner mercenaries were also part of the "unmarked" Russian troops that deployed and annexed Crimea (Dinu 2022).

In Syria, Wagner routinely took part in extortions and civilian massacres, all with the tacit approval of the Syrian government. Their prominence continued to grow as they helped the army of the ill-equipped regime retake its territory, especially from the terrorist organization Islamic State. In 2017, four Russian mercenaries savagely beat a Syrian army deserter to death and filmed the murder, the instrument of torture and murder being a sledgehammer (McBride 2022).

In February 2018, the organization attempted to consolidate its status as a leading combat force by attacking a U.S. Special Forces outpost in eastern Syria. Several hundred Wagner mercenaries along with Syrian government forces attacked thirty American Special Forces members and their allies in the Syrian Democratic Forces (SDF). Their action was not successful because the Wagner group and Syrian regime troops suffered significant losses of military equipment and human lives, and on the American side the casualties were zero, with only one SDF soldier injured (McBride 2022).

Taking advantage of the power vacuum created in the wake of the Arab Spring, Wagner deployed forces in North Africa in support of warriors aligned with their

geopolitical (national) or private interests. Mercenaries played a role in the second Libyan civil war, fighting for General Khalifa Haftar when the rival government tried to storm the capital Tripoli. A report by Human Rights Watch stated that the group has indiscriminately placed mines across the country, which continues to affect locals (McBride 2022).

The Wagner group's reputation has grown amid its engagement in African nations such as Mali, Sudan and the Central African Republic. The organization has been linked to several massacres in the Central African Republic, to the point where the United Nations has begun to investigate their links to civilian executions (McBride 2022). In Mali, Wagner supported the military junta, which was beneficial to Russia's interests, amid Russian arms government demands and diplomatic support to stop human rights groups' investigations into large-scale crackdowns on dissidents. Wagner has also been linked to civilian massacres in Mali (Dinu 2022).

Beyond previous actions in other regions of the world, the issue of terrorism committed by the Wagner group has really come to the attention of international opinion with the outbreak of war in Ukraine in 2022. The media periodically publishes information about the crimes of these mercenaries and their processes, the most conclusive example being the situation in Bucha in the spring. From the very first days, Ukraine blamed Russia's 64th Motorized Infantry Brigade, which was based in Bucha. According to communications intercepted by German intelligence services, Russian mercenaries from the Wagner Group (McBride 2022) were also involved.

In November 2022, the head of Russia's private military group Wagner defended a brutal video that apparently shows the death of a mercenary who defected to Ukraine. Putin's ally Yevgeny Prigozhin said the unverified footage of 55-year-old Yevgeny Nuzhin being hit with a sledgehammer was "the death of a dog for a dog". The convicted murderer announced in September that he had switched sides to the Ukrainians (BBC 2022).

3. Terrorism in Russian - Controlled Areas

We have previously pointed out that acts of terrorism are a method for the Kremlin regime to solve the problems related to the preservation of power, eliminating potential enemies and resolving conflicts. On the evolution of terrorism, the study "Ukraine Russia crisis: terrorism briefing" conducted by The Institute for Economics & Peace (IEP)[1] in March 2022, provides important data, for example on

[1] The Institute for Economics & Peace (IEP) is an independent, non-partisan, non-profit think tank dedicated to reorienting the world's focus towards peace as a positive, achievable and tangible measure of human well-being and progress. The IEP achieves its objectives by developing new conceptual frameworks to define peace, providing values for measuring peace and discovering the relationships between business, peace and prosperity, and promoting a better understanding of the cultural, economic and political factors that create peace.

the evolution of terrorism against the background of Russia's conflicts with Georgia in 2008 and with Ukraine in 2014.

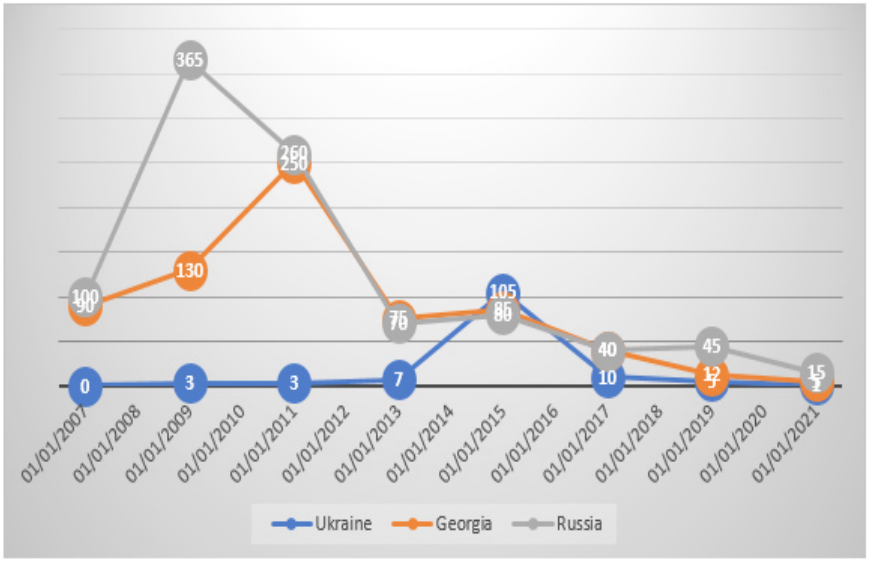


Figure no. 1: Terrorist attacks in Ukraine, Georgia, Russia, between 2007 and 2021
(Data analysed by The Institute for Economics & Peace were obtained from Dragonfly TerrorismTracker, IEP calculations)

As seen in Figure no. 1, terrorism in the three countries has decreased over the last six years under review. By 2016, 93% of terrorist attacks had taken place. The peak period took place around 2010, following the Russian-Georgian conflict.

The same study names the Shariat Jamaat group (also known as Vilayat Dagestan[2] and associated with Chechen and Ingush separatist actions), and its affiliates, as responsible for most terrorist attacks, most of them on the territory of the Russian state. The Dagestan Front is part of the terrorist group Emirate of the Caucasus.

The potential for terrorism in Ukraine and Georgia is also determined by the violent demonstrations. The same study of the IEP presents the following data:

[2] Dagestan Front of the Armed Forces of the Caucasus Emirate.

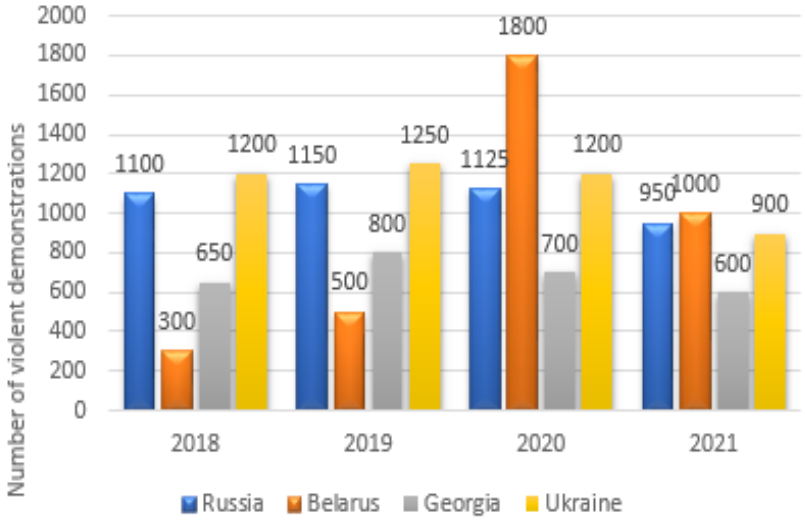


Figure no. 2: Violent demonstrations in Ukraine
and Belarus between 2018 and 2021
(Data taken from Ukraine Russia crisis: terrorism briefing
conducted by The Institute for Economics & Peace (IEP), March 2022, p. 5.)

Despite a regime that aimed to eliminate any form of opposition, most of the violent demonstrations took place in Russia. In fact, in 2021, Russia, Ukraine and Belarus were the countries in the region that each recorded around 1,000 violent demonstrations. In the case of Belarus, the reason for the demonstrations was opposition to the regime of Alexander Lukashenko, which has been in power for over 25 years. The violent demonstrations in Ukraine resulted from the fact that the population no longer wanted a regime under Moscow and, after the government of President Volodymyr Zelenskyy took office, they were fuelled by conflicts in Donetsk and Luhansk (Peace 2022).

The main finding of the data presented is that the number of terrorist acts increases with the intensity of conflicts. Both the Georgian conflict of 2008 and the Ukrainian conflict in 2014 saw substantial increases in terrorist activity around the wars, and as the current war intensifies, terrorist activity is likely to intensify as well.

The share of attacks by terrorist groups operating in the Eurasian region, including in states listed as under Russian influence, is shown in Figure no. 4.

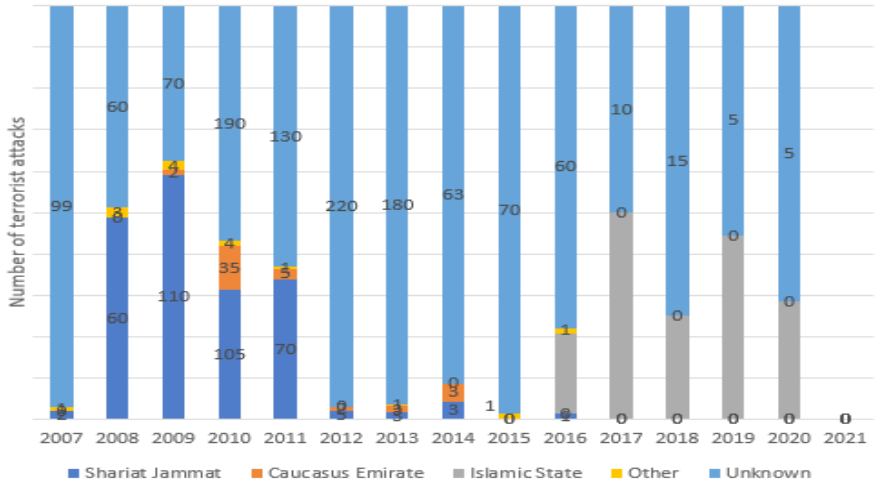


Figure no. 3: Number of attacks by terrorist groups
in Russia and Eurasia region, 2007-2021
(Data analysed by The Institute for Economics & Peace, p. 4)

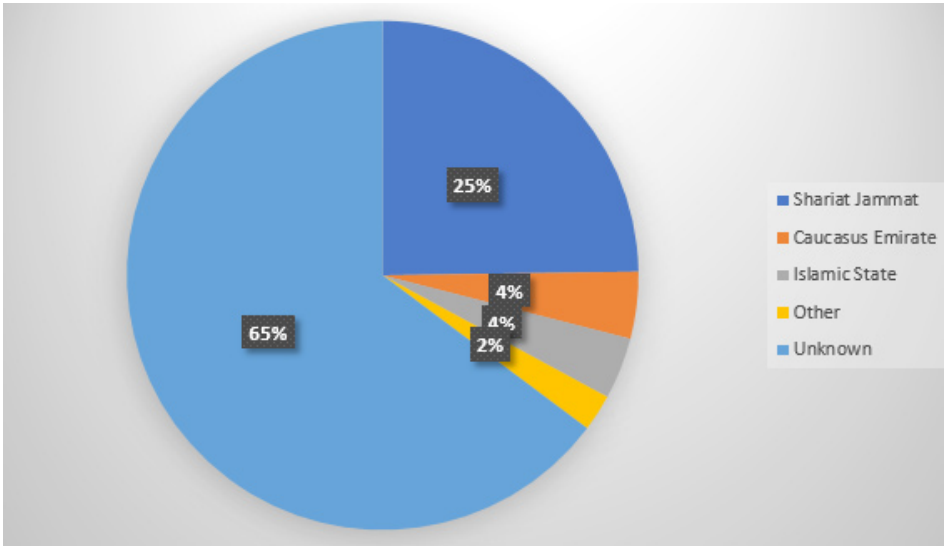


Figure no. 4: Share of terrorist attacks in Russia
and Eurasia region, 2007-2021
(Data analysed by The Institute for Economics & Peace, p. 4)

Remarkably, most terrorist attacks in the Eurasian region are carried out by unknown groups. As their share is very high, over 65%, more suspicions arise.

They may be unorganized groups, different from known terrorist groups acting in a certain context. Another reason could be that the terrorist actions belong to the Russian state itself, all the more so as we have shown the terrorist actions of the Wagner group.

With the Russian invasion of Ukraine, mercenaries from the Middle East, primarily Syria and Libya, have been enlisted in the Russian army. This fact has not been hidden by the Russian authorities, Russian Defence Minister Sergei Shoigu said during a meeting of the Russian Security Council on March 11 that "more than 16,000 people from the Middle East volunteered to join Russian forces" (Brylov, Denis 2022), and Russian President Vladimir Putin has said they must be supported and helped to cross into the territory where hostilities are taking place (BBC 2022). Also, in March 2022, the Ukrainian General Staff reported on the possible recruitment by Russia of approximately a thousand militants from Syria and the Lebanese organization Hezbollah. The only condition for recruitment was experience in urban combat. The danger brought by these fighters is that it was not the desire to fight against Ukraine that was the basis of their decision to enlist, but the desire to enter member countries of the European Union (Brylov, Denis 2022).

The Syrian Observatory for Human Rights said that at least 40,000 Arab mercenaries have been enlisted, of which 22,000 were part of the Russian armed forces and about 18,000 as part of the Wagner Group. At the same time, in recent weeks, about 700 troops of the 25th Special Forces Division, known in Syria as the "Tiger Force", under the command of General Suheil al-Hassan, have left for Russia (Mroue 2022). Ukrainian authorities confirmed that about 500 mercenaries from Libya and Syria participated in the hostilities in the Luhansk and Donetsk regions. Some of these forces were destroyed by the Ukrainian army on April 18, 2022 (In the east, the Armed Forces destroyed a detachment of Libyans and Syrians - Danilov 2022).

As the few available studies show, the subject of Islam and Muslims in the Russian military remains controversial. First of all, military sociologists indicate a constant level of religiosity in the army: in 1990, 14% of the military considered themselves believers, in 1992 – 22%, in 1996 – 34%, then in 2006 – already 68% (Brylov 2022). Some of these religious people are radicalized and can pose a real terrorist threat, not only in the Eurasian area, but also in Europe.

4. Russia's Terrorist Danger against the European Union

Russia's aggression is hybrid: it includes not only a military component, but also a religious, political and economic one. In essence, by attacking Ukraine, Putin has created an instrument for the comprehensive destabilisation of Europe that weakens

and divides the European geopolitical model without harming Russia. Such a threat to Europe has not existed since the end of the Second World War.

Attacks in previous years, such as the Paris attacks of 12 November 2015, have shown the EU's vulnerability to terrorism. In this attack, all three foreign fighters known to the authorities were able to escape surveillance and transmute from and to Europe and Syria unnoticed. Therefore, although they have been identified as a threat to state security and French citizens, the supervisory bodies failed to locate them on Belgian and French territory. This would have allowed security services to raise the alert level, and possibly prevent attacks. According to Turkish authorities, Turkey notified France twice of the presence on its territory of the suicide bomber Mostefai, in December 2014 and June 2015, but received no feedback from Paris (Ray 2022).

The Kremlin is recruiting mercenaries from the Middle East to be sent to war in Ukraine. When war crimes are committed, the mercenaries can be blamed for them, and when the mercenaries die, there is no obligation of the Russian state to pay pensions and no reaction of revolt in Russia from the families of the victims of the war in Ukraine (Brylov 2022). There are also opinions that Russia is destroying Ukraine just as it has destroyed Syria. In 2016, Russian troops virtually destroyed Aleppo, one of Syria's oldest cities and its cultural capital. In Syria, the Russian army has committed crimes against humanity. Today, they are committing the same crimes in Ukraine (Serban 2022).

Thus, at present, Russia presents several types of hybrid dangers, and the war in Ukraine represents a direct terrorist threat to European security. Moreover, as we have previously shown, Putin wants to destabilise Europe as much as possible, cause chaos and recession, and he is willing to go to any lengths to win as much as possible in the war in Ukraine, even if that means supporting war crimes.

Russia's terrorist threat is also an indirect one. Putin has created large-scale risks of a resurgence of terrorism in the Caucasus. In addition to the risk of a terrorist threat and further socio-political destabilisation, there will inevitably be the discrediting of Muslims around the world. Kadyrov sends the Chechens to wage an invasion war in Ukraine, while presenting it to his troops as a just cause (Kuczyński 2022).

Russia's historical relationship with terrorism, the use of terrorist actions to solve power problems and the use of the Wagner Group on several fronts of interest demonstrate that this country has no reluctance taking terrorist actions whenever it has an interest. The question is whether the European Union is able to cope with Russia's terrorist attacks on several fronts and whether the population of European countries would show solidarity in the fight against Russian terrorism, all the more so as there is a great deal of frustration amid the energy crisis.

Conclusions

In its desire to become a great global power again, Russia also includes elements of terrorism in its actions. Putin has used terrorist attacks, even with dangerous chemical and biological agents, radioactive substances, to oust his opponents. In order to gain influence, he has collaborated with terrorist groups or other dictators who in turn have used terrorism to gain or maintain power. Moreover, he founded the Wagner Group, made up of people with radical orientations who, more often than not, underlie the ideologies behind various terrorist groups.

All of the above listed would not present such a threat to the security of the democratic world, if terrorism had not for a long period of time had a different meaning for Russia than in the free world, respectively of an instrument of power.

Russia poses an indirect terrorist threat by engaging heavily radicalised Muslims into the war. Even if they are not used by the Russian state, they themselves can organise themselves into terrorist groups that fight for their own state or religious interests. The revitalisation of Islamist terrorism in Europe not only means a deterioration of security in this area, but it can also lead to an escalation of the smouldering conflicts in the Balkans.

The conclusion is that Russia has the means and has shown that it is capable of carrying out terrorist actions when its power interests demand it. We have shown that most of the acts of terrorism in the Eurasian region belong to unknown terrorist groups and this, together with the hybrid war against the West, is a major risk to Europe's security.

BIBLIOGRAPHY:

Analysis, SOVA Center for Information and. 2010. "The Structure of Russian Anti-Extremist Legislation." Accessed on November 12, 2022. https://www.europarl.europa.eu/meetdocs/2009_2014/documents/droi/dv/201/201011/20101129_3_10sova_en.pdf

BBC. 2022. "Putin Spoke on Sending 'Volunteers' from the Middle East to Ukraine." *BBC News*. Accessed on November 2, 2022. https://www.bbc.com/russian/news-60707686

BBC. 2022. "Ukraine war: Wagner chief Prigozhin defends brutal killing video." *BBC News*. Accessed on November 4, 2022. https://www.bbc.com/news/world-europe-63623285

Blackmore, Erin. 2020. "How the Red Terror set a macabre course for the Soviet Union." *National Geografic*. Accessed on November 4, 2022. https://www.nationalgeographic.com/history/article/red-terror-set-macabre-course-soviet-union.

Borshchevskaya, Anna. n.d. *The russian war of war.* Editor Washintgton Institute. Accessed on November 3, 2022. https://www.washingtoninstitute.org/media/352

Brylov, Denis. 2022. "Muslim Legions" of the Russian Army – English version." *Observatoire International du Religieux* Bulletin nr.7. Accessed on November 18, 2022. https://obsreligion.cnrs.fr/bulletin/muslim-legions-of-the-russian-army-english-version/.

Brylov, Denis. 2022. "Muslim Legions" of the Russian Army." *Observatoire International du Religeux.* Accessed on November 2, 2022. https://obsreligion.cnrs.fr/bulletin/muslim-legions-of-the-russian-army-english-version/

C.Walters, Robert J.FischerEdward P.HalibozekDavid. 2019. "Terrorism: A Global Perspective." *Introduction to Security* 401-412. Accessed on November 6, 2022. doi:https://doi.org/10.1016/B978-0-12-805310-2.00016-0.

2022. „Cum schimbă relațiile internaționale declararea Rusiei ca „regim terorist"." *Europa Liberă.* Accessed on November 12, 2022. https://romania.europalibera.org/a/rusia-regim-terorist/32112541.html

Dinu, Clarice. 2022. „Ce este Grupul Wagner, armata privată a lui Putin, care l-ar avea ca țintă pe Volodimir Zelenski." *Hot News.* Accessed November 17, 2022. https://www.hotnews.ro/stiri-razboi_ucraina-25397673-este-grupul-wagner-armata-privata-lui-putin-care-avea-tinta-volodimir-zelenski.htm.

Filipov, David. 2017. "Here are 10 critics of Vladimir Putin who died violently or in suspicious ways." *Washington Post.* Accessed November 18, 2022. https://www.washingtonpost.com/news/worldviews/wp/2017/03/23/here-are-ten-critics-of-vladimir-putin-who-died-violently-or-in-suspicious-ways/.

Getty, J. Arch. 2002. "Excesses Are Not Permitted": Mass Terror and Stalinist Governance in the Late 1930s." *The Russian Review* 113-115.

Holroyd, Matthew. 2021. "Was Russia behind the killing of Zelimkhan Khangoshvili? A Berlin court says yes." *euronews.* Accessed November 2, 2022. https://www.euronews.com/my-europe/2021/12/15/zelimkhan-khangoshvili-russian-man-convicted-of-2019-berlin-murder-of-georgian-chechen.

HotNews.ro. 2022. „Rusia, declarată stat care sponsorizează terorismul – rezoluție a Parlamentului European." *HotNews.ro.* Accessed November 23, 2022. https://www.hotnews.ro/stiri-razboi_ucraina-25921076-rusia-declarata-stat-care-sponsorizeaza-terorismul-rezolutie-parlamentului-european.htm.

2022. „În est, Forțele Armate au distrus un detașament de libieni și sirieni - Danilov." *Platformă multimedia de limbi străine a Ucrainei.* Accessed November 3, 2022. https://www.ukrinform.ua/rubric-ato/3463326-na-shodi-zsu-znisili-zagin-livijciv-ta-sirijciv-danilov.html.

Kuczyński, Grzegorz. 2022. "Why Ukraine War Matters For Chechnya's Kadyrov." *Ukraine Monitor.* Accessed November 14, 2022. https://warsawinstitute.org/ukraine-war-matters-chechnyas-kadyrov/.

Laskowska, Katarzyna. fără an. *TERRORISM IN RUSSIA – MECHANISMS.* BSP_ Book.indb. Accessed November 5, 2022. https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/2026/1/BSP_10_2011_Laskowska.pdf.

McBride, Julian. 2022. "Wagner Group: The Case for a Terrorist Designation." *Geopolitical Monitor.* Accessed November 16, 2022. https://www.geopolitical monitor.com/author/julianmcbride/.

Mroue, Bassem. 2022. "Syrian fighters ready to join next phase of Ukraine war." *APNews.* Accessed November 4, 2022. https://apnews.com/article/russia-ukraine-putin-islamic-state-group-syria-europe-4ede428219450a58b0439912bc43cc15.

Newman, Scot. 2021. "Russia Fatally Poisoned A Prominent Defector In London, A Court Concludes." *NPR.* Accessed November 3, 2022. doi:https://www.npr.org/2021/09/21/1039224996/russia-alexander-litvinenko-european-court-human-rights-putin.

Orenstein, Mitchell A. 2019. "Russia's Hybrid War on the West." *Oxford Academy* C2–C2.P73. Accessed November 16, 2022. doi:https://doi.org/10.1093/oso/9780190936143.003.0002.

Peace, The Institute for Economics &. 2022. *Ukraine Russia Crisis: Terrorism Briefing.* IEP. Accessed November 12, 2022. https://www.economicsandpeace.org/wp-content/uploads/2022/03/Ukraine-Russia-Terrorism-Briefing-web.pdf.

Rahman-Jones, Imran. 2017. "Why does Russia support Syria and President Assad?" *BBC News.* Accessed November 2, 2022. https://www.bbc.com/news/newsbeat-39554171.

Ray, Michael. 2022. "Paris attacks of 2015." *Britannica.* Accessed November 16, 2022. https://www.britannica.com/event/Paris-attacks-of-2015.

Rupar, Terri. 2014. "Remember when a Ukrainian presidential candidate fell mysteriously ill?" *Washington Post.* Accessed Octomber 18, 2022. https://www.washingtonpost.com/news/worldviews/wp/2014/03/12/remember-when-an-ukrainian-presidential-candidate-fell-mysteriously-ill/.

Serban, Teodor. 2022. „"Măcelarul din Alep" a ordonat bombardamentele care au distrus Harkovul. Cine este generalul rus care preferă muniția interzisă. Acest text a fost cop "Măcelarul din Alep" a ordonat bombardamentele care au distrus Harkovul. Cine este generalul rus care pre." *ziare.com.* Accessed November 18, 2022. https://ziare.com/general-rus/general-rus-macel-alep-siria-ordin-bombardamente-harkov-1740891.

Toader, Alexandru. 2022. „SUA nu consideră necesar să declare Rusia drept „stat terorist". Motivul invocat de americani." *Știrile ProTV.* Accessed December 2, 2022. https://stirileprotv.ro/stiri/international/sua-nu-considera-necesar-sa-declare-rusia-drept-zstat-terorist-motivul-invocat-de-americani.html.

DOI: 10.53477/ 1842-9904-22-17

INFORMATION OPERATIONS – COMPARATIVE DOCTRINAL ANALYSIS

Cosmina-Andreea NECULCEA*
Florian RĂPAN, PhD**

The aim of this article is to identify differences in doctrinal projection at the level of the North Atlantic Alliance. The article has been designed as a comparative study of the doctrinal projections specific to information operations (InfoOps), mainly with regard to the doctrines and operations manuals of the United States of America, as the originator of most of these documents, NATO doctrines and domestic doctrines. On an initial examination of the three doctrinal projections, it can be observed that there are differences in the InfoOps approach, both in terms of surface elements, recognized by identifiable markers, and differences in perspective, which allow and encourage interpretation. There is therefore a need to clarify the nature of InfoOps and its correct understanding from a conceptual and practical point of view, and to achieve coherence between the doctrines for information operations of NATO member states and the allied doctrine.

Keywords: *information operations (InfoOps); doctrines; comparative analysis; differences; doctrinal interoperability.*

*
* *

In writing the article, we started from identifying the differences in doctrinal projection in the American, Romanian and NATO doctrinal apparatuses, with the intention of contributing to a higher degree of interoperability for joint actions and exercises in the field of information operations. To this end, we have resorted to a content analysis of the information operations doctrines and, subsequently, to a

**** LT Cosmina-Andreea NECULCEA is Assistant Lecturer at "Henri Coandă" Air Force Academy, Braşov and a PhD Student at "Carol I" National Defence University, Bucharest, Romania, E-mail: saghincosmina@yahoo.com***
***** Maj. Gen (Ret) Florian RĂPAN, PhD, is a Professor at the "Dimitrie Cantemir" Christian University, Bucharest, Romania, E-mail: rapan_florian@yahoo.com***

comparison of them from three perspectives: the definition of the concept and key areas, the identification of the operating principles and of functional structure and the surface and in depth differences in the application of each of the key areas of information operations within the American, the Romanian and NATO doctrines.

Introduction

Over time, the nature of conflicts has changed, and one of the determining factors of warfare and the one that led to the shaping of concepts was *technology*. In the past, differences between the technological capabilities of adversaries constituted the main differentiating element and, together with the level of asymmetry regarding the number of belligerents involved in the conflict, were essential for gaining superiority. Nowadays, the extensive flow of information, the decrease in the number of soldiers involved in operations (decrease in the battlefield deployment density), as well as the influence of technology, have made the achievement of information superiority, which can only be interpreted in classic operations, the main objective. In addition to the five operational domains, land, air, maritime, space and cyber, the human mind can be considered a new domain of operations (even if it has not become an independent domain, the cognitive domain is being recognized in the Western armies as well; in Chinese doctrine it is enacted as such). For example, the US Information Operations Doctrine, JP 3-13/ Information Operations, emphasizes the importance of human influence and gives the cognitive dimension the status of the most important dimension of the information environment.

At the Alliance level, AJP-3.10/ Allied Joint Doctrine for Information Operations, published in 2015, emphasizes the influence of global trends on the human factor and global power dynamics, creating instability and increasing the probability of conflict. The importance and complexity of the information environment, as well as the changing nature of global security, has led NATO to continuously develop and adapt its concepts and doctrines to meet new challenges.

In the Romanian doctrinal projection, InfoOps[1] support Joint Operations, being considered the most appropriate response to contemporary threats.

1. InfoOps Definitions in NATO, US and Romanian Doctrinal Projections

The rapid changes that have taken place in the information environment, the experiences on the battlefield as well as the lessons learned from recent conflicts have determined the member states of the Alliance to focus more and more on the

[1] For the coherence of the current article and the assurance of its conceptual unity, we will preserve the abbreviation InfoOps, as it appears within the Romanian doctrines.

concept of *information operations* and the awareness of their importance. Concern over InfoOps policies and doctrines both at the level of the Alliance and at the level of other nations began in the 1990s, when many military operations were assigned InfoOps objectives.

The US, as the originator of most Alliance doctrinal documents, first addressed the operational context of InfoOps in the US Field Manual FM 100-6/ Information Operations, which outlined the continuing expansion of the media and assessed that "this new era, the so-called Information Age, offers unique opportunities as well as some formidable challenges". (Headquarters, Departament of the Army 1996, iv). In 1998, the first doctrine for information operations in a joint context, JP 3-13/ Joint Doctrine for Information Operations, emerged and information operations received a definition very similar to what is understood today by operations in cyberspace. Information warfare was also described as "information operations conducted during time of crisis or conflict (including war) to achieve or promote specific objectives against an adversary or adversaries". (Joint Chiefs of Staff 1998, I-1) The emergence of a new doctrine, in 2006, led to the abandonment of the use of the term *information warfare* in favour of the term *information operations* and introduced the concept of *information environment*.

According to the 2006 doctrine, the main objective of InfoOps was "to achieve and maintain information superiority for the US and allies" (Joint Chiefs of Staff 2006, ix), in order to "enhance commanders' freedom of action and enable them to make decisions and maintain the initiative while remaining inside the adversary's decision cycle" (Joint Chiefs of Staff 2006, 1-5). The current doctrine projects information superiority only in relation to information assurance/IA[2]. In both doctrines, the information environment is described as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act upon information" (Joint Chiefs of Staff 2014, ix) and includes three dimensions: physical, informational and cognitive, which constantly interact with individuals, organizations and systems.

The InfoOps approach from the US perspective is slightly different from NATO or Romanian because it does not offer a definition, but rather considers the information operations to be "the integrated employment, during military operations, of information-related capabilities/ IRCs in concert with other lines of operation to influence, disrupt, corrupt, or impede decision-making of adversaries and potential adversaries while protecting our own" (Joint Chiefs of Staff 2014, ix). Information capabilities are "tools, techniques, and activities that affect any of the three dimensions of the information environment" (Joint Chiefs of Staff 2014, x)

[2] "Information assurance is necessary to gain and maintain information superiority", (JP 3-13/2014, p. II-9). Here, information superiority represents "The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same".

and are available to the commander to affect the three dimensions of the information environment.

In Alliance operations, InfoOps played a special role, a role that was analyzed and reflected both in theoretical works and in doctrines and manuals, implying direct effects on the battlefield. For NATO, a common understanding of information operations seemed to be crucial to meet the challenges. In this context, AJP-3.10/ Allied Joint Doctrine For Information Operations, published in 2009, defined information operations as follows: "Info Ops is a military function to provide advice and coordination of military information activities in order to create desired effects on the will, understanding and capability of adversaries, potential adversaries, and other NAC approved parties in support of Alliance mission objectives". (NATO Standardization Agency 2009, 1-3)

In order to define influencing operations, the above description was completed by another expression, information activities, defined as "...actions designed to affect information and or information systems. They can be performed by any actor and include protective measures." (NATO Standardization Agency 2009, 1-3). Six years later, a new allied doctrine AJP-3.10/2015 appears, which no makes substantial changes to the definitions in the previous doctrine.

At the national level, the concept of information operations was implemented in the Romanian Army in 2006, with the emergence of the Doctrine of Information Operations, which aimed to create a general framework for planning, conducting and evaluating the effects of information operations, at the operative and tactical level. Later, in 2011, a new doctrine appeared, the Doctrine for Information Operations of the Romanian Army (General Defence Staff 2011), which aimed to align with the 2009 NATO document. The emergence of new types of threats, such as the hybrid one, led modern armies, and implicitly the Romanian Army, to formulate new responses. Therefore, in 2017, a new doctrine emerges, which is still in force today, the Information Operations Doctrine, which emphasizes the role and importance of information operations in the contemporary operating environment. The definition of information operations is very similar to the allied doctrine: "a general staff function, intended for the analysis, planning, evaluation and integration of all information activities in order to obtain the desired effects on the will, understanding, perception and capabilities of adversaries, potential adversaries and of the target audiences approved by the Supreme Council of National Defence, in support of the fulfillment of military objectives". (General Defense Staff 2017, 13)

Considering the comparative analysis of InfoOps definitions from a diachronic perspective, we can assert that InfoOps remains a complex subject, which needs a clear and concise understanding. For example, while the definition of InfoOps in the American doctrine limits InfoOps coordination and synchronization only

during military operations, the definitions of the other two projections analyzed do not specify this. In the American conception, InfoOps relies on other information capabilities to create effects at a specific time, in and through the information environment, giving the commander the ability to gain an operational advantage. While these IRCs create their own effects, InfoOps represents the aggregation of these effects, an action seen as essential to achieving objectives.

While NATO and Romanian doctrines mention, in a general way, that the purpose of InfoOps is to create the desired effects, the American definition is much more specific, the purpose of InfoOps being to influence, disrupt, corrupt, usurp the decision-making of adversaries and potential adversaries. Taking into account the three dimensions of the information environment, the cognitive effects manifested by behavior modification are the most important for achieving decisive results, but take time to manifest, compared to effects in the physical and informational dimensions, which can be immediate.

The continuous evolution of the information domain makes it more necessary than ever the need to constantly update these definitions to guarantee a clear vision of what the complexity of InfoOps means. At the same time, different definitions in the three doctrinal projections will lead to different interpretations, and these interpretations can lead to strategic failures.

2. InfoOps Principles in the NATO, US and Romanian Doctrinal Projections

Underpinning the planning and conduct of information operations is a set of principles that have the role of directing activities with an impact on the information environment in support of the full range of military operations, as well as integration into the target selection process.

The Information Operations Doctrine presents a number of ten principles that constitute the foundation of planning and conduct of information operations, principles that are largely taken from the 2009 NATO doctrine, with some modifications or additions.

A first difference identified is that the allied doctrine includes a set of nine principles, while at national level the initial set of nine principles has been completed with the tenth, adaptability. It is also observed that the principles are not listed identically, with principles 7 and 8 changing places.

Moreover, the 2015Allied Doctrine for Information Operations stands out with a different set of principles, compared to the previous doctrine, as can be observed in the Table no. 1:

Table no. 1: InfoOps Principles based on Romanian and NATO doctrines

No.	Doctrine of Information Operations/ 2017	AJP-3.10/ Allied Joint Doctrine for Information Operations/ 2009	AJP-3.10/ Allied Joint Doctrine for Information Operations/ 2015
1.	Comprehensive approach to the operation	Effects-Based Approach to Operations	Focussed and integrated
2.	Commander's directions and his personal involvement	Commander's Direction and Personal Involvement	Coherent and consistent
3.	Permanent coordination and synchronization	Close Coordination and Sequencing	Comprehensive understanding
4.	Accuracy of intelligence on which the decisions are based	Accurate Intelligence and Information	Centralized planning and decentralized execution
5.	Centralized planning and decentralized execution	Centralised Planning and Decentralised Execution	Continuous
6.	Contribution to the joint target management process	Input to Joint Targeting	Monitoring and assessment
7.	Continuity	Early Involvement and Timely Preparation	Agility
8.	Early involvement and timely preparation	Continuity	-
9.	Monitoring and evaluation of effects	Monitoring and Assessment	-
10.	Adaptability	-	-

One of the durable components of the doctrine is represented by the principles, because they stand for the basis of the management of military operations and must be applied on a large scale, regardless of the operational context. One could argue that once we find different principles in doctrines, this can also be understood as a simple conceptual gap. This analysis of differences in the projection of information operations principles are identifiable markers or surface elements in comparative doctrinal analysis.

3. Key Domains Coordinated within InfoOps According to NATO, US and Romanian Doctrinal Projections

Falling under the same category of surface elements, the key domains differ to a greater extent between the conceptual apparatuses analyzed. The first difference concerns precisely the naming/framing of the list of activities under the InfoOps umbrella. The Romanian doctrine of information operations projects a series of 12 key domains**:** Psychological Operations (PSYOPS), Troop Presence, Profile and Posture (PPP), Operations Security (OPSEC), Information Security (INFOSEC), Military Deception (MILDEC), Electronic Warfare (EW), Physical Destruction, Key

Leader Engagement (KLE), Military Engagement, Cyberspace Operations, Cyber Defence and Civil-Military Cooperation (CIMIC), subordinated and coordinated within InfoOps, and can be considered "InfoOps activities only when they are directly aimed at the understanding and perception, will and capabilities or means of the adversary, the potential opponent or other approved entities". (General Defence Staff 2017, 22)

NATO Doctrine, AJP-3.10/2015 includes key InfoOps domains in a distinct category, entitled Capabilities and Techniques Integrated Through Information Operations. Although the list is not exhaustive, the capabilities and techniques listed represent the basis of most InfoOps activities. The current doctrine has also completed the list of capabilities in the previous doctrine with three other capabilities, such as Special capabilities, Military Public Affairs and Cultural understanding and engagement and excluded Information Security/INFOSEC. (NATO Standardization Office 2015, 1-10)

In the US, JP 3-13/ Information Operations doctrine of 2014, lists a more numerous series of capabilities that contribute to InfoOps, which fall under Relationship and Integration**,** as follows: Strategic Communication, Interagency Joint Coordination Group, Public Affairs, Civil-Military Operations, Cyberspace Operations, Information Assurance, Space Operations, Military Information Support Operations/MISO (in previous editions of the doctrines, Psychological Operations, Intelligence, Military Deception, Operations Security, Special Technical Operations, Joint Electromagnetic Spectrum Operations, Key Leader Engagement (Joint Chiefs of Staff 2014, II-5).

The second difference stems from differences in terminology. This includes both surface elements, directly identifiable markers in terms of the name alone, but also aspects of depth or differences of perspective in terms of the philosophy and physiognomy of the key domains involved. Regarding the psychological operations, with the acronym PSYOPS, used by most NATO states, in 2011, there was a terminological change at the US level, replacing the acronym PSYOP with MISO (Military Information Support Operations). However, this change did not produce considerable effects. According to Lieutenant Colonel Robert Bockholt, spokesperson for the US Special Operations Command, "PSYOP forces conduct MISO", and "Psychological operations refer to the name of units, while MISO refers to the function that the military personnel in PSYOP units perform". (Myers 2017)

Furthermore, compared to mass media operations and information and public relations activities, PSYOPS have control over the content and the means of disseminating information and, implicitly, involve a focus on influencing activity through them, i. e. on achieving certain expected effects of the transmitted contents. For example, the Russian InfoOps approach to information security aims not only to guarantee the technical integrity of information, but also to produce the intended

cognitive effect. Russia also focuses on influencing the perceptions of the target audience, whereas the Western countries are rather constrained by the objectivity of information. (Joan Prats i Amorós 2019, 16) These examples allow the understanding of the issue as a result of the difference in perspective to a greater extent than as a result of the simple difference in surface, i. e. naming.

Two key domains that encompass the offensive and defensive aspects of InfoOps in cyberspace are *cyberspace operations* and *cyberdefence*. The term cyber is also used in the American doctrinal projection, under the name *cyberspace operation*s, while at NATO level, the 2009 doctrine remained at the wording of *computer network operations* (attack, exploitation and defence), and the 2015 doctrine is limited only to *computer network attack* and *computer network exploitation.*

Through electronic warfare/EW, armies try to dominate the electromagnetic spectrum through the three types of EW actions: electronic protection, electronic attack and electronic support. The US equivalent of EW consists of joint electromagnetic spectrum operations/JEMSO which involves both electronic warfare actions and joint management operations of the electromagnetic spectrum. (Joint Chiefs of Staff 2014, II-12)

While Alliance doctrine, AJP-3.10/2015 and Romanian doctrine use the term Civil-Military Cooperation/CIMIC, the US uses the term Civil-military operations/ CMO and does not accept the idea that this action dimension, civil-military cooperation, is considered a capacity.

Regarding key leader engagement/KLE, this capability appears in all three doctrinal projections analyzed, and in the NATO and Romanian projections, it also appears at the military level. In carrying out the mission, every military interacts with the local population, which imposes the need for one's training regarding the mode of interaction as well as the messages to be disseminated. The link between *strategic communications/*StratCom and KLE is that engaging StratCom requires "a robust Key Leader Engagement programme" (Gage 2014, 54). This concept benefits from rather poor documentation and there are no established standards for what a successfully completed KLE would mean.

Another important aspect of information activities is presence, posture and profile/PPP. The deployed unit(s) must be aware of the public image they are displaying, regardless of the deployment area or the assigned mission. In the American projection, this capacity is not included in the list, but we find aspects related to it in the attempts to define StratCom, a capacity that does not only mean "verbal communication, it is presence, posture and profile of our activities, particularly our readiness to support our words with actions thus showing our strength from the political level down until very tactical". (TŪTINS 2015)

In the Romanian doctrine, PPP ranks second in the set of key domains coordinated within InfoOps. The perception and attitude of the target audience can

be influenced by the presence, attitude and behavior of the troops and their leaders. The PPP description also emphasizes the need to synchronize these aspects with media operations, given the role of commanders in conveying messages, as well as the protection requirements of forces deployed in the field. Allied doctrine places PPP within the set of capabilities and techniques integrated through information operations, highlighting at the same time the individual effect that this capability can create, because "the mere presence of a force can have a significant impact on perceptions", but also on the information environment. (NATO Standardization Office 2015, 1-12)

Even if the OPSEC concept emerged relatively late, the semantic content is very old, being a means of protection whose challenge "is not the release of classified information, but rather pieces of a puzzle that provide adversaries with a picture of the overall operation" (Dominique 2009, 17). All three doctrinal projections analyzed emphasize the importance of OPSEC in preventing the accidental leakage of information, as well as the role of this capacity in the protection of one's own information. OPSEC requires constant attention, and this capability must be integrated into all aspects of military operations from the very planning stage. In addition, OPSEC proves very important when it comes to deception. The two areas prove to be essential in achieving surprise as well as obtaining and maintaining initiative. Although OPSEC and MILDEC are distinct and discrete processes, the two domains support each other. This is highlighted in all three projections analyzed, each of which clearly highlights this relationship in the text of the doctrine. The link between the two domains stems precisely from their purpose, namely affecting the opponent's decision-making process. Although history provides many examples of deception, military success does not depend entirely on deception. Rather, it serves as a force multiplier. The recent changes in the socio-political landscape have not only increased the importance of deception, but also require Western countries to step up their game of deception. For example, the Russian military sees deception as a distinct activity, outlined by the term Maskirovka (Vowel 2016) – a much more complex form of enemy deception.

The only kinetic lever, as Călin Hentea mentioned, is the physical destruction, a leverage used "not only to eliminate or annihilate some points or command networks or adverse communications, but also to achieve a certain psychological impact on the targeted population or leaders". (Hentea 2008, 303)

The definition of IA/Information Assurance captures the role of this capability in achieving and maintaining information superiority, as well as the interdependence between IA and cyber operations. Also, many features of IA are attributed to Information security/ INFOSEC. With the recognition of space and cyberspace as two new operational domains, the physiognomy of warfare has also changed. Space can be used for both peaceful and aggressive purposes, and the potential for conflict in space has never been more apparent.

Regarding the connection of space operations with information operations, perceived as a joint function, the American doctrine states that the two support each other. Outer space supports the flow of information, it also supports the decision-making process, but it can also deliver information to the information environment. On the other side, information can generate effects that support the achievement of information superiority, defined as "the degree of control in space of one force over any others that permits the conduct of its operations at a given time and place without prohibitive interference from terrestrial and space-based threats". (Joint Chiefs of Staff 2020, I-4)

Conclusions

An essential prerequisite for achieving the objectives entrusted to us is the ability of armies to train and operate together in an integrated and coordinated manner. This helps to guarantee operational efficiency that can only be achieved through a controlled approach to interoperability. In this context, doctrines represent the basic pillar that includes both the concepts (what?) and all the rules of engagement and aspects that characterize military action (how?). In other words, doctrines describe the methods, organization as well as the set of procedures that make it possible to carry out actions in a joint framework. Therefore, comparing different InfoOps approaches is an essential process in the effort to ensure doctrinal coherence.

The nature of InfoOps must be continually clarified so that information operations are conceptually and practically well understood and to be consistent with the evolution and trends of the modern battlefield. There is also a need to achieve coherence between NATO and allied doctrines for information operations. For example, as long as the degree of doctrinal correspondence between NATO and Romanian doctrines in the field of information operations is quite high, interoperability can be achieved seamlessly. Instead, the Romanian presence in information operations under American command would create problems regarding, for example, the integration of INTEL within this function. We can say that interoperability at the operational and tactical level also depends on this issue, on the doctrinal differences, both at the surface level (principles and key areas) and at the depth level, as a way of application and subordination in relation to the joint command. Regarding the three doctrinal projections, there are significant differences, both in the umbrella term "information operations" and in the key areas. Therefore, we emphasize the need to revise the related terminologies in order to be able to keep up with the characteristics of the contemporary operating environment, or to complete the doctrinal apparatus with documents necessary to obtain a high degree of interoperability in joint Romanian-American exercises. It is not necessary

to change the terminology used, as it is compatible with NATO terminology, but only to identify these forms of coordination in order to obtain a higher coefficient of doctrinal interoperability, respectively to introduce other concepts necessary for understanding the functionality and dynamics of the battlefield into the Romanian doctrinal apparatus, such as that of Effects-Based Approach to Operations, a proposal found as early as 2016 in the study Information Warfare (Lesenciuc 2016, 47-51). Last but not least, an update of the Romanian Army Doctrine would allow an easier adaptation to the realities of the battlefield.

BIBLIOGRAPHY:

Dominique, Michael. 2009. "Information Operations: The Military's role in gaining information superiority." https://duckduckgo.com/?q=dominique+michael+information+operations+the+military+role+in+gaining+site%3Aapps.dtic.mil&t=newext&atb=v344-1&ia=web

Gage, Daniel. 2014. "The continuing evolution of Strategic." *The Three Swords Magazine*, 54. https://www.jwc.nato.int/images/stories/threeswords/NOV_STRATCOM_evolution.pdf

General Defence Staff. 2006. *Doctrina Operațiilor Informaționale.* (*Information Operations Doctrine).*

—. 2017. *Doctrina Operațiilor Informaționale.* Ediția a 2-a. (*Information Operations Doctrine)*

—. 2011. *Doctrina pentru Operații Informaționale a Armatei României.* (*Doctrine for Information Operations of the Romanian Army*).

Headquarters, Departament of the Army. 1996. "FM 100-6 Information Operations." https://www.hsdl.org/?view&did=437397

Hentea, Călin. 2008. "Noi dimensiuni ale războiului contemporan." *Revista Română de Sociologie*, 289-306. https://www.revistadesociologie.ro/pdf-uri/nr.3-4-2008/Art%206-Hentea.pdf (*New dimensions of contemporary warfare)*

Joint Chiefs of Staff. 1998. *Joint Pub 3-13 Joint Doctrine for Information Operations.* https://www.c4i.org/jp3_13.pdf

—.2006. *Joint Publication 3-13 Information Operations.* https://www.globalsecurity.org/intell/library/policy/dod/joint/jp3_13_2006.pdf

—. 2014. *Joint Publication 3-13 Information Operations.* https://irp.fas.org/doddir/dod/jp3_13.pdf

—. 2020. *Joint Publication 3-14 Space Operations.* https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14Ch1.pdf

Lesenciuc, Adrian. 2016. *Războiul Informațional.* Brașov: Editura Academiei Forțelor Aeriene "Henri Coandă". (*Information Warfare*)

Myers, Meghan. 2017. "The Army's psychological operations community is getting its name back." https://www.armytimes.com/news/your-army/2017/11/06/the-armys-psychological-operations-community-is-getting-its-name-back/

NATO Standardization Agency. 2009. *AJP-3.10 Allied Joint Doctrine for Information Operations.*

NATO Standardization Office. 2015. *AJP-3.10 Allied Joint Doctrine for Information Operations.* Edition A, Version 1.

Prats i Amorós Joan, Guillaume-Barry Augustin. 2019. "Not Only Blood. The Need to Integrate Psychological Operations in the West's Military Culture." *Opinion Paper IEEE 81/2019*, 16. https://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEE81_2019JOAPRA_Psyops_ENG.pdf

TŪTINS, Māris. 2015. "Strategic Communication and Protecting Environment in Military Training Areas." http://putniadazos.lv/sites/default/files/kcfinder/files/2015-05-05_StratCom_environment.pdf

Vowel, JB. 2016. "Maskirovka: From Russia, With Deception." *Real Clear Defense.* https://www.realcleardefense.com/articles/2016/10/31/maskirovka_from_russia_with_deception_110282.html

DOI: 10.53477/1842-9904-22-18

WAR IN UKRAINE: RUSSIAN PROPAGANDA THEMES

Dana Ionela DRUGĂ*

With this article, we aim to identify the propaganda themes associated with the Russian Federation in the context of the war in Ukraine and how they are formulated, based on an analysis of the articles found in the database of EUvsDisinfo (Disinfo Database) over a two-month period (August−September 2022). Propaganda themes were identified by applying two types of research: qualitative (content analysis and thematic analysis) and quantitative. The research results indicated the following Russian propaganda themes: the theme of the Zaporozhye nuclear power plant attack, the theme of Nazism and fascism, the theme of military aggression, the theme of Russian values and legality (referendum), the theme of lost sovereignty and imperialism, the theme of staging attacks/massacres, the theme of the global conspiracy and the West, the theme of the food crisis/food insecurity, the theme of Russian minority and Russophobia. The purpose of this analysis is to increase awareness regarding Russian Federation's hostile actions in the virtual space, as well as the resilience of users to online messages.

***Keywords**: Russian Federation; propaganda; disinformation; Ukraine; war in Ukraine; Central and Eastern Europe*.

Introduction

The aggressive actions of the Russian Federation in Ukraine are not only taking place on the ground, but also in the information space, through propaganda and disinformation. By propaganda we mean "the systematic dissemination of ideas, theories, opinions with a political purpose, especially to win the masses over to the side of power" (Voicu 2018, 12). Closely related to propaganda, disinformation is defined by those "false or distorted information that have been carefully constructed,

**** Dana Ionela DRUGĂ is a PhD Student at the "Mihai Viteazul" National Intelligence Academy, Bucharest, Romania. Email: druga.dana@animv.eu***

being secretly introduced into the adversary's communication system in order to deceive either decision-makers or public opinion" (Voicu 2018, 11). The link between the two briefly defined concepts resides in the fact that propaganda includes disinformation, seen as an action to manipulate/persuade a target audience in order to advance political objectives; in other words, disinformation can be considered a tool of propaganda, aiming to attack/denigrate/criticize actors on the international stage.

Throughout this paper, we will use the phrase *propaganda messages* with reference to the Russian Federation, precisely to illustrate and encompass the totality of information distortion actions, through falsification or biased presentation of them, based on multiple purposes (attracting the public, legitimization of aggressive military actions, etc.).

In the article, we aim to achieve the following objectives: the analysis of Russian propaganda themes by identifying, in the database of EUvsDisinfo (Disinfo Database), articles present on various Russian propaganda websites, directed against Central and Eastern Europe states, the USA and NATO and EU organizations; identifying the targets of Russian propaganda; identification of websites that disseminate propaganda messages and their investigation (presence on social media, number of followers, interactions with users in the online environment); detection of propaganda themes applicable to the identified states/organizations, based on the disinformation messages investigated.

1. Methodology and Steps to Obtain the Research Results

The types of research used were qualitative analysis (by analyzing messages thematically) and quantitative analysis. For the present research we used open sources, namely the EUvsDisinfo[1] database, which deals with the identification of disinformation messages of the Russian Federation. We chose this database because it provides relevant information and data and is one of the largest sources of information on the area of research interest, having indexed and identified over 14,000 disinformation messages from international and[2] national /local[3]media. The EUvsDisinfo project was developed in 2015, by the East Group StratCom of the European External Action Service, to better forecast, address and respond to Russian Federation's propaganda campaigns affecting the European Union, its Member States and countries in the common neighborhood. The main objective of EUvsDisinfo is to increase awareness and understanding of the Kremlin's propaganda operations

[1] Available at https://euvsdisinfo.eu/disinformation-cases/

[2] As described on the web page, About section, https://euvsdisinfo.eu/about/#

[3] national / local media we mean those publications / news that reproduce local events/situations, in the language of the respective state, without having international visibility. For example, The New York Times is visible internationally, compared to the publication Gazeta de Sud, which is a regional newspaper.

and to help citizens in Europe and beyond develop resilience to propaganda and manipulation (EUvsDisinfo).

After selecting the database, we applied *criteria to narrow the search*, depending on: (1) the states/organizations that show interest in the research problem and (2) the period under research. For this purpose, Central and Eastern Europe countries[4], NATO and EU organizations and the USA were selected. We believe that the US is relevant in the current context, as it has shown its economic and diplomatic support to Ukraine since 2014, being the most important donor of humanitarian assistance to Ukraine. According to the US State Department since 2014, the United States has provided approximately $900 million in humanitarian assistance to vulnerable communities in Ukraine (www.state.gov). For this reason, we appreciate that it is obviously a target of propaganda messages in the context of the war in Ukraine. In terms of the period under investigation, we have chosen the period August 01−September 30, 2022. We have chosen this period from the perspective of the current events of the war in Ukraine, namely: the expansion of strategic and military objectives by the Russian Federation, with reference to the Kherson and Zaporizhia regions; the preparation of the referendum on the illegal annexation of the four regions in the south and east of Ukraine (Donetsk, Luhansk, Zaporozhye, Kherson); decreeing partial mobilization in the Russian Federation on September 21, 2022.

After identifying the database and applying narrowing search criteria, 158 messages disseminated by Russian propaganda sites resulted. We specify that certain sites could not be accessed, especially those disseminated by RT/Sputnik in the European Union, due to restrictions and the closure of those sites.

Data coding and organization

For the organization and structuring of the data, we have divided each propaganda message according to the state and/or organization targeted by the respective messages: Ukraine; US; EU; NATO; West; states from Central and Eastern Europe.

Criteria for analyzing Russian propaganda messages

After the data organization stage, we applied several criteria for message analysis:

− *Criterion of distribution of propaganda messages* was chosen to investigate the most active social media sites/platforms/channels in terms of the spreading Russian propaganda messages;

− the language/content rendering criterion was applied to investigate the role of Russian language in the context of dissemination of propaganda messages, starting from the idea that Russian speakers and ethnic Russians can be more easily influenced based on information sent in their native language;

[4] The states were included in the research considering the definition proposed by the Organization for Economic Cooperation and Development for the states in the CEEC area – Central and Eastern European Countries.

– *the criterion of social media presence* of websites disseminating propaganda messages was chosen to analyze the potential for amplification and dissemination of Russian propaganda messages;

– *State/supra-state criterion:* the messages were analyzed and grouped according to the states and/or organizations targeted by propaganda messages (for example, Ukraine, Poland, US, NATO, EU). We used this criterion to observe the dynamics and preponderance of targeting a certain state in the region by the Russian Federation;

– *The thematic criterion* pursued the investigation of propaganda themes, resulting in nine Russian propaganda themes targeting Central and Eastern Europe states, in the context of the war in Ukraine.

2. Research Results

In this section, we present the research results, grouped on two dimensions: quantitative and qualitative. Thus, the quantitative dimension will indicate the total number of propaganda messages identified, as well as the most active sites/platforms through which the respective messages were disseminated. The qualitative dimension will focus on the thematic analysis of propaganda messages.

The quantitative dimension

The results of the research related to the quantitative dimension record 158 propaganda messages disseminated through 116 channels (sites/social media platforms).

• *Online platforms and number of messages disseminated*

As the size and objectives of the work do not allow us to analyze all the sites/platforms identified in the database – 116, we will consider the four most active sites identified in the EUvsDisinfo database, according to the number of messages disseminated in the selected period. Thus, we identified the following sites: (1) arabic.rt.com, (2) nabd.com, (3) RIA Novosti, (4) oroszhirek.hu. In the following, we will analyze each of these sites/platforms to indicate the number of messages disseminated, the states and the targeted organizations.

Arabic.rt.com disseminated the most propaganda messages (18) during the selected period, and the messages targeted Ukraine, the US and Europe/EU. As other studies show (Oweidat 2022), Russian propaganda in the Middle East through *arabic.rt.com* is very active, as there are several conditions that provide the opportunity for the Russian Federation to advance its foreign policy: firstly, amid historical distrust of Western news sources, the Russian Federation presents its own media as a better alternative to other Arabic-language networks and has a more receptive audience in the region than in the West.

Nabd.com disseminated 12 propaganda messages during the selected period and they targeted Ukraine, Europe/EU, the US. Nabd is a free app/platform that allows access to the latest news based on each user's personalized feed. The platform has taken the messages shared by RT into its content.

RIA Novosti disseminated 11 propaganda messages during the selected period; it is a press agency in the Russian Federation, believed to be the promoter of official Russian propaganda messages. The messages are directed against Ukraine and the European Union. It should be noted that, at this moment (November 2022), the agency's page cannot be accessed in the European Union states.

Oroszhirek.hu has promoted nine pro-Russian propaganda messages, targeting Ukraine, Poland, Romania, the European Union, and the US.

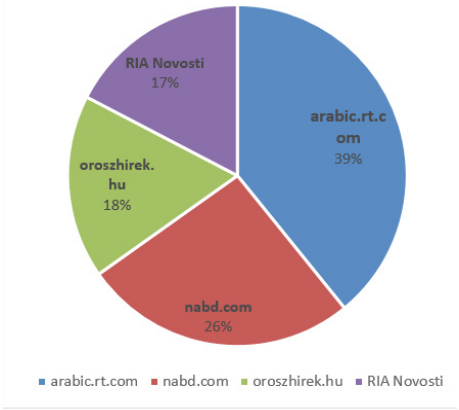


Figure no. 1: Distribution of propaganda messages according to the websites/platforms identified

• *The language criteria*

The language criterion was applied to identify the states and audience category to which Russian propaganda messages are addressed. Thus, of the 116 sites/platforms identified, Russian is the predominant language, followed by Arabic, Hungarian and Spanish. Propaganda messages in the Russian language and about *the Russian World* (*ruskiy mir*) are particularly aimed at countries with significant Russian-speaking minorities. The purpose of using the Russian language in advancing propaganda messages is to create and deepen the connection between these communities and the Russian Federation, by encouraging the self-identification of citizens of other states with Russia. This category includes countries such as Latvia, Estonia, Ukraine, Lithuania and Moldova, where Russian-speaking communities represent between 4 and 25% of the population (Coolican 2021, 6).

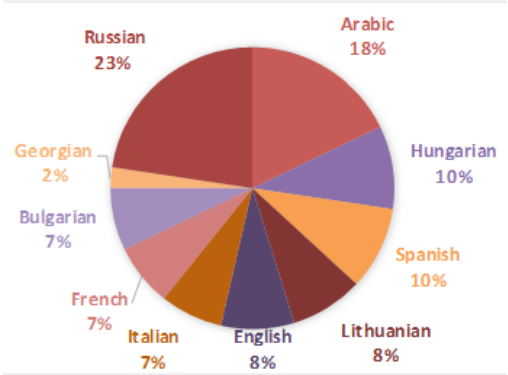


Figure no. 2: Language criteria of propaganda messages

• *Potential for amplifying propaganda messages depending on social media activity/presence of identified sites*

We consider it important to investigate this aspect in order to understand the connection between the propaganda messages used and the number of platforms that can be targeted for exploitation. Therefore, within highly digitized societies within which a multitude of platforms are used, they are inevitably exposed to greater risk due to the diversity of messages that can be used to reach a wider audience. (Bokša 2019, 2)

Orszhinek.hu is present on the Facebook/Meta, Twitter, VKontakte, Telegram and YouTube. Note that the website has also been ranked by other researchers as being among the most influential in Hungary in terms of the impact of messages on the population (Bartha 2018) and as a source of disinformation (Šuplata 2016). *Arabic.rt.com* is present on almost all social media platforms: Facebook, Instagram, TikTok, Twitter, Telegram, VKontakte, Rutube, YouTube. *RIA Novosti*, the press agency controlled by the government of the Russian Federation, had at the beginning of October 2022 more than 2.2 million followers on Facebook and Instagram, millions of subscribers on Telegram, followers on TikTok, subscribers on VKontakte and Rutube. The *Nabd.com* platform is also present on Facebook, Twitter and Instagram.

Table no. 1: Social media presence of the identified sites

Platform	Arabic.rt.com	RIA Novosti	Orszhinek.hu	Nabd.com
Facebook (Likes/Followers)	15,000,000	2,200,000	160,000	1,700,000
Twitter (followers)	5,000,000	No data available	1,400	300,000
Instagram	1,600.000	1,000,000	-	288,000
YouTube	2,500	-	-	-
Rutube	1,000	30,000	-	-
VKontakte	100,000	3,000,000	1,200	-
TikTok	1,000	1,000,000	-	-
Telegram	30,000	2,000,000	12,000	-

• *State criterion*

Regarding the 158 messages identified in the EUvsDisinfo database, the most (156) targeted Ukraine, followed by the US, EU, NATO, Poland.

Table no. 2: Russian propaganda messages and targeted states/organizations

Targeted state/ organization	Examples of Russian propaganda messages	Number of propaganda messages in which each state/organization was mentioned
Ukraine	"Ukraine is a non-sovereign state, ruled either by the US or other European states." "Ukraine supplies grain to European states in exchange for weapons and is responsible for the food crisis in Africa." "Ukraine is committing atrocities against its own people." "Ukraine plans to attack Zarapozhie nuclear power plant ." "Ukraine is a Nazi, corrupt, terrorist state dependent on the US."	**156**
US	"US Develops Biological Weapons on Russia's Border." "The US and the West are waging a hybrid war against Russia in Ukraine." "The US and Britain have created their own army in Ukraine."	**61**
EU	"EU sanctions hurt Europe more than Russia." "EU citizens ask it to stop supporting Ukraine." "Europe has become a US military and political colony." "Fascist EU sanctions against Russia prove that European countries are no longer democratic."	**50**
NATO	"NATO is creating the pretext for a world war." "NATO is directly involved and is on the Ukrainian side." "Soldiers fighting under the Ukrainian flag are citizens of NATO member states."	**16**
Poland	"Poland plans to impose control over agriculture and other sectors of Ukraine's economy." "Poland will annex territories from Ukraine."	**10**
Romania	"Ukraine controls territories that belong to other countries. Ukraine exists within unnatural borders. Transcarpathia should be ceded to Hungary, Galicia to Poland, Bucovina to Romania, Donbass and Crimea to Russia."	**2**
Letvia	"Russian citizens are segregated in public transport in Riga."	**3**
Hungary	"The head of the European Commission threatened Italian, Hungarian and Polish citizens."	**3**
Moldavia	"Moldova decided to ban flights to Moscow, under pressure from Kiev."	**1**

Source: EUvsDisinfo Review

Qualitative dimension – thematic analysis of Russian propaganda messages

After selecting and organizing the studied messages in the database, the next step was to identify recurrent themes, to which the propaganda messages found in the EUvsDisinfo database were subsumed. For this, we identified the frequency of occurrence of key terms in the titles of the propaganda messages, in the following form: nuclear/Zaporozhe, Nazism/fascism, military aggression, referendum, lost sovereignty, massacre, conspiracy, food crisis/food insecurity, Russian minority/ Russophobia.

We have chosen thematic analysis because it is a type of qualitative research, which allows the investigation and analysis of a large set of data. It is a research method through which themes identified in a data set can be identified, analyzed, organized and described (Braun and Clarke 2006). Thematic analysis is also useful for summarizing key features of a large data set and helps the researcher structure the data to produce an organized paper (King 2004). In the present case, the propaganda messages found on EUvsDisinfo were structured in the form of themes, detailed below. A theme is an abstract entity that gives meaning and identity to a recurring experience and its varied manifestations. As such, a theme captures and unifies the nature or basis of experience into a meaningful whole (King, 362). In the context of the war in Ukraine, the identification of propaganda themes facilitates our understanding of the Russian Federation's foreign policy strategy and objectives.

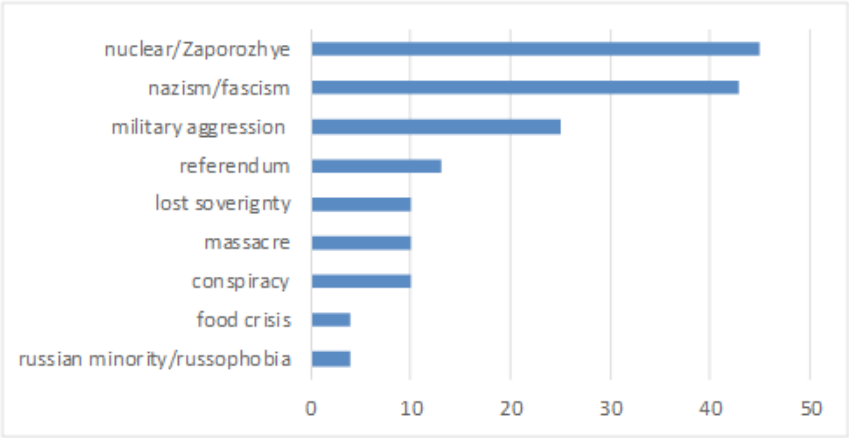


Figure no. 3: Frequency of key terms, subsumed by propaganda themes

Thus, we identified nine themes of Russian propaganda messages, as follows**:** (1) *the theme of the nuclear attack –Zaporizhia power plant;* (2) *the theme of Nazism and fascism;* (3) *the theme of military aggression;* (4) *the issue of Russian values and legality (referendum);* (5) *the theme of lost sovereignty and imperialism;* (6*) the theme of staged attacks and massacres;* (7) *the theme of global conspiracy and the West;* (8) *the theme of food crisis/insecurity;* (9) *the theme of Russian minority and Russophobia.*

The theme of the nuclear attack – the Zaporizhye plant

Zaporizhia nuclear power plant is a central point of interest for Russian propaganda, with messages targeting Ukraine or Western states. The Russian Federation's rhetoric on the nuclear issue is repetitive and emphasizes the Russian

state's immediate readiness to use nuclear weapons. However, the intent of use can only be at the declarative level, with the ultimate goal being to induce fear among the population. The impact of these threats is based on the Russian Federation's extensive network of influence in other states, which perpetuates the nuclear rhetoric. (Arndt and Horovitz 2022)

This propaganda narrative that Ukrainian forces want to destroy the Zaporozhye nuclear power plant is designed to distract the public from the real perpetrators of war atrocities. Ukrainian authorities have accused the Russian Federation of dangerous actions that could cause a nuclear catastrophe. (EUvsDisinfo)

In a report dated August 3, 2022, the Institute for the Study of War (ISW, 03/08/2022) believes that Russian forces are exploiting the general fear of a nuclear disaster in Ukraine in order to diminish the military support offered by Western states to the Ukrainian army. At the same time, the director general of the International Atomic Energy Agency (IAEA), Rafael Grossi, declared on August 3 that the nuclear power plant in Ukraine, which is currently occupied by Russian forces, is "completely out of control" and that "all principles of nuclear security have been violated" (Lederer, August 3, 2022). Subsequently, the EU High Representative, Joseph Borrell, in a Twitter postdated August 6, 2022[5], condemned Russia's military activities in Zaporozhye and labeled them as a serious and irresponsible violation of nuclear security rules and another example of Russia's non-compliance with international norms.

The theme of Nazism and fascism

Concepts related to World War II, Nazism and fascism are used by the Russian Federation to accuse Ukraine of being ruled by Nazi leaders. The importance of World War II as a symbolic resource of nation-building has been noted by some scholars. (Malinova 2014) The accusation of "fascism/Nazism" is a way of appealing to the values of the Russian population, who associate World War II with fascist horrors and crimes. (Cottiero, și alții 2015)

The fascist label has been attached to the Ukrainian government and Ukrainian soldiers by Russian media since 2014, in the context of ultra-nationalist movements in the Euro Maidan protests. Through Russian propaganda messages, Ukraine is repeatedly referred to as a Nazi country and as using symbols of Nazism. In a Russian propaganda show, a video was broadcast [6]showing white crosses, which the broadcast considered to be Nazi symbols on Ukrainian army tanks. In reality, the white crosses shown in the video are not Nazi symbols. Such crosses were often depicted on the flags of various Cossack regiments. (EUvsDisinfo, 09/08/2022, No. 308) Unlike

[5] Available at https://twitter.com/JosepBorrellF/status/1555858270589538305

[6] Available at https://all-make.net/polnyj-kontakt-s-vladimirom-solovyovym-ot-08-09-2022.html - (between 01:06:05 and 01:06:27)

these white crosses, the German crosses on tanks and other military equipment were distinct. In reality, crosses of various colours and shapes are widespread symbols in Christian nations around the world. They are present during religious ceremonies and are present on national flags and coats of arms or in other spheres of public life. (EUvsDisinfo, 09/08/2022, no. 308)

The theme of military aggression

Military aggression is attributed in particular to NATO, which is considered to be directly involved in the war in Ukraine. This is a recurring Russian propaganda narrative, which claims that Alliance forces are directly involved in the "special military operation". Both before and during the war in Ukraine, disinformation messages have sought to distort NATO's image and reputation both within member states and abroad. These messages are an attempt to justify Russian military failures and to downplay the role of the Ukrainian armed forces, presenting the military conflict as a war with NATO. (EUvsDisinfo)

The theme of Russian values and legality (referendum)

While in other themes previously developed, the messages discredited or were in a negative register, the propaganda messages that support the actions and foreign policy lines of the Russian Federation consider it to be the liberating state of the Ukrainian territories. These narratives portray the Russian Federation as a liberator state, conducting legitimate military actions.

In the context of holding referendums, the Russian Federation is trying to justify the annexation of Ukrainian territories by claiming that the inhabitants of these regions want to join the Russian Federation freely and that the referendum is legal (a view presented by sites such as bgr.news-front.info). This is an attempt to legitimize its illegal military control and aims to forcibly change Ukraine's borders, in violation of the UN Charter and the independence, sovereignty and territorial integrity of Ukraine. (EUvsDisinfo) At the same time, through this narrative, Russian propaganda seeks to manipulate public opinion regarding the reality of the unfolding of events. In reality, voters are being coerced into voting, the BBC reports. The EU High Representative, Joseph Borrell, condemned the decision to hold a referendum, stating that the EU would not recognize "these illegal votes" as they do not express the free will of the people living in these regions. Other messages supporting the actions of the Russian Federation emphasize that it strictly respects humanitarian law and only strikes military targets, or that the military actions are in full compliance with the UN Charter.

Another propaganda narrative that attempts to emphasize the superiority of Russian culture and language is that by which Russia claims that it must purify the Ukrainian language by eliminating totalitarian and terrorist influences and that the Ukrainian language is an artificial creation (EUvsDisinfo).

The theme of lost sovereignty and imperialism

Within this theme, the US, NATO and the EU are discredited and portrayed as sovereign over other states within the European Union. Another state with imperial ambitions is considered to be Poland. Through propaganda messages, Ukraine's statehood and independence is contested, presenting Poland as a country with imperial ambitions. Also, messages about the Western strategy to create a joint Poland-Ukraine state, disseminated by websites such as ukraina.ru, RIA, geworld.ge, have also been identified. We believe that the objective of these propaganda narratives is to create a sense of distrust between Ukraine and Poland and other Western states supporting Ukraine.

As for Ukraine, Russian propaganda messages claim that it has lost its sovereignty and the country's president is under the control of other political leaders in France, Germany or the US. (belvpo.com, 08/31/2022)

Theme of staging attacks/massacres

This is a recurring theme through which Russian propaganda messages attempt to relativize the actions of the Russian military in Ukraine. These messages are an attempt to deflect responsibility from the Russian Federation for the massacres committed by the Russian armed forces during the occupation of the Kharkov region, actions proven by forensic teams and witnesses. (EUvsDisinfo)

Contrary to this propaganda theme, not only Ukrainian soldiers, but also several civilians were tortured and execute. A similar pattern has been observed in other areas under Russian occupation. On September 23, the UN Commission of Inquiry on Ukraine presented its conclusions, after investigations in four regions: Kyiv, Kharkov, Sumy and Chernihiv; from these it appears that the Russian Federation committed multiple war crimes during the invasion.

The theme of global conspiracy and the West

The global conspiracy theme is an inherent element of the Russian propaganda system, having a negative impact on critical thinking skills by undermining the public's trust in objective information, leading to low resilience to propaganda. For example, in the present research, we have identified a conspiratorial message[7] that portrays a global elite inciting ethnic conflict to save its decadent hegemony. This is a recurring Russian propaganda narrative that seeks to discredit liberal democracies by claiming that the latter are in reality systems run by "globalist elites" and "shadow governments" that subjugate and manipulate the masses by disintegrating communities and by deepening ethnic divisions in society. (www.geopolitika.ru) The article's message about Western elites' supposed subservience to "international financiers" is also consistent with recurring pro-Russian propaganda

[7] Available in Italian at https://www.geopolitika.ru/it/article/latlantismo-sbagliato-memoria-di-darya-2

narratives about all-powerful global elites or secret elites who rule the world and control political leaders.

Another topic identified within this theme is built around the assassination of Daria Dughina, a context in which the Western secret services, along with Ukraine, are accused of plotting and her assassination. Messages have been disseminated by sites such as *www.svpressa.ru* and *www.geworld.ge*

The theme of food crisis/insecurity

Under this theme, Russian propaganda messages claim that the economic sanctions imposed on the Russian Federation in the context of the war of aggression against Ukraine caused the food crisis. In reality, Moscow is responsible for the global food crisis as a result of the war in Ukraine: the naval blockade of Ukrainian ports, the bombing of transport infrastructure and the bombing of food storage facilities. The Russian Federation's invasion of Ukraine has serious consequences for global agriculture and food security. Russian media and officials attempt to deflect attention from the Russian Federation's responsibility for increasing global food insecurity. (US Department of State 2022)

The worsening food crisis due to the war has also generated intense concerns at European level. The President of the European Council, Charles Michel, said at the World Food Security Summit in September 2022 that "food security is the main challenge facing the world today. The current world food crisis is exacerbated by Russia's war against Ukraine". (www.consilium.europa.eu)

"The Russian Federation is instrumentalizing the food crisis and launching propaganda and disinformation messages for ideological purposes, using the mass media and diplomats' speeches" (Mario Morales, Diálogo, 2022). Russian warships are blockading Ukrainian ports in the Black Sea, preventing grain exports, posing a risk to global food supply chains. The invasion of Ukraine by Russia has generated a global food crisis that could last for several years. (UN, 2022)

The Russian invasion of Ukraine has destabilized global food markets and driven up food prices due to increased costs of production, transportation and cargo insurance. At the same time, the Russian Federation has attacked and destroyed substantial food stocks. In reality, EU sanctions are directed against the Russian government, financial sector and economic elites, and target the Russian Federation's ability to finance military aggression. Russia's agricultural sector is not targeted. The US also exempts transactions in food, agricultural products and medical supplies from sanctions (EUvsDisinfo).

The theme of the Russian minority and Russophobia

Against the backdrop of protecting the Russian minority, Russian propaganda actively promotes messages justifying its aggressive military actions, including

the invasion of Ukraine, or accusing other states of violating human rights and the Russian-speaking minority. For example, in this research, we identified a disinformation message about public transport in Riga (Latvia), according to which Russian citizens are segregated in public transport and are not allowed to sit in the front rows of public transport. These disinformation messages were promoted by sites such as *sport24.ru* or *ren.tv.* Therefore, Latvia is accused of violating the human rights of the Russian-speaking minority, although the managers of the transport company in Riga (Rigas Satiksme) have denied the information and qualified the action as provocation. (Myth Detector, September 2022)

Another type of message identified in the current research is subsumed under the same type of argumentation, according to which Russian citizens are discriminated: in schools in Ukraine, students would be taught to report their parents and children to tell the teacher if the family has relatives in Russia and if the parents speak Russian. This type of message has been disseminated on various pro-Russian websites: *donpress.ru*[8]; *rg.ru* , as well as on the Twitter platform. According to the disinformation message, children are encouraged to immediately report if their parents watch Russia TV programs if their parents talk negatively about Ukraine's President Volodymyr Zelensky.

Conclusions

Currently, in Ukraine, Russian propaganda is directed not only against the Ukrainian state, but also against Central and Eastern Europe states, as well as NATO, the EU and the US. The main difference from the pre-war period is that the entire propaganda system is much more active in disseminating propaganda and disinformation messages. Through the Internet (social media platforms, mass media, online channels), the Russian Federation promotes propaganda messages in the context of the war in Ukraine with the aim of changing the perception of the internal and external public regarding the unfolding events, but also with the aim of creating the appearance of legitimacy of its actions, including through the instrumentalization of visual content from the online environment. The Russian Federation aims to (re) assert the Russian identity in the public space, sending discrediting messages to Western nations and trans-Atlantic structures in the context of the war in Ukraine.

BIBLIOGRAPHY:

Arndt, Anna Clara, and Liviu Horovitz. 2022. "Nuclear rhetoric and escalation management in Russia's war against Ukraine: A Chronology." *International Security Research Division.* Accessed on 04.09.2022 https://www.swp-berlin.

[8] The disinformation message is available at: https://donpress.ru/v-ukraine-prosjat-detej-donosit-na-roditelej/

org/publications/products/arbeitspapiere/Arndt-Horovitz_Working-Paper_Nuclear_rhetoric_and_escalation_management_in_Russia_s_war_against_Ukraine.pdf

Aronson, J. 1994. "A Pragmatic View of Thematic Analysis." *The Qualitative Report* 1-3.

Bokša, Michal. 2019. "Russian Information Warfare in Central and Eastern Europe: Strategies, impact, countermeasures." *German Marshall Fund.*

Braun, V., and V Clarke. 2006. "Using thematic analysis in psychology." *Qualitative Research in Psychology* 3 (2): 77-101. https://doi.org/10.1191/1478088706qp063oa.

Coolican, Sarah. 2021. *The Russian Diaspora in the Baltic States: The Trojan Horse that never was.* LSE IDEAS. Accessed in September 2022. http://eprints.lse.ac.uk/114500/1/Coolican_the_trojan_horse_in_the_baltic_states_published.pdf.

Cottiero, Christina, Katherine Kucharski, Evgenia Olimpieva, and Robert Orttung. 2015. "War of words: the impact of Russian state television on the Russian Internet." *Nationalities Papers* 43 (4): 1-23. doi:10.1080/00905992.2015.1013527.

Gorenburg, Dmitry. 2019. *Russian Foreign Policy Narratives.* Marshall Center, available at https://www.marshallcenter.org/en/publications/security-insights/russian-foreign-policy-narratives-0, Accessed on 09/04/2022.

King, N. 2004. "Using templates in the thematic analysis of text." In *Essential Guide to Qualitative Methods in Organizational Research* , by C. Cassels and G Symon, 256-270. London: Sage.

Malinova, Olga. 2014. "The idea of a common past in post-Soviet Russia: ideas about nation and imperial heritage." *Muzeum Historii Polski* 263-282.

Oweidat, Nadia. 2022. "The Russian Propaganda in Arabic Hidden from the West." *Fikra Forum*, April. Accessed in September 2022. https://www.washingtoninstitute.org/policy-analysis/russian-propaganda-arabic-hidden-west

Hey, Marian. 2018. *Matryoshka of liars. Fake news, manipulation, populism.* Bucharest: Humanitas.

EUvsDisinfo Review - https://euvsdisinfo.eu/

Myth Detector - https://mythdetector.ge/

Council of Europe - www.consilium.europa.eu

UN. 2022. "The war in Ukraine and its impact on local and global food security". https://www.undp.org/ukraine/blog/war-ukraine-and-its-impact-local-and-global-food-security?utm_source=EN&utm_medium=GSR&utm_content=US_UNDP_PaidSearch_Brand_English&utm_campaign=CENTRAL&c_src=CENTRAL&c_src2=GSR&gclid=Cj0KCQiAyracBhDoARIsACGFcS7LXNyKfdMNbGdBs7BP6X91L4xhBWRiUG8CN04imIsYQHu3DvWfsTcaAhuzEALw_wcB

Institute for the Study of War (ISW). 2022. Report 03/08/2022. https://www.understandingwar.org/sites/default/files/Russian%20Operations%20Assessments%20August%203.pdf

SCIENTIFIC SEMINAR

"Consolidated National Defence – Fundamental Concept of Operation for the Romanian Army 2021-2024"

October 28th, 2022

Today's security environment is characterised as dynamic, unstable, unpredictable and complex. Under these circumstances, the country's defence transcends the sphere of the military establishment responsibility. Thus, Romania faces a wide range of new threats and cannot take a unilateral approach to ensure its security, but must act as part of collective – regional or global –security. Creating a stable security environment, by increasing resilience to threats of all forms, will give Romania the chance to benefit, unhindered, from the tremendous development opportunities that will contribute significantly to increased national well-being and prosperity.

Therefore, this year's Scientific Seminar on "*Consolidated National Defence – Fundamental concept of operation for the Romanian Army 2021-2024*" was organised online by the Centre for Strategic Defence and Security Studies on 28 October 2022.

The event aimed at debating the fundamental concept of operation for the Romanian Army, starting from the military risks and threats to Romania, the Army's missions and the national military objectives, with a time horizon 2021-2024.

The scientific event marked this time, through the topics addressed, the major concern about security at national and regional level, as well as the common interest in developing inter-institutional and international cooperation in the field of security and defence at the allied level, being shaped by the participation of important structures with concerns in the field, subordinated to the Defence Staff: Doctrine and Joint Training Directorate, Operations Directorate, Land Forces Staff and Air Force Staff, representatives from the Multinational Division South-East (MND-SE) and researchers from the CDSSS. There were also present Romanian collaborators, specialists, experts, researchers and academic staff from the "Carol I" National Defence University.

The main issues addressed, on which discussions were held, were those regarding:

- "*The role of the Romanian Army doctrine in the defence planning process*";
- "*The Concept of Consolidated National Defence*";
- "*The role of integrated air defence within the concept of consolidated national defence*";
- "*Mission of the Multinational Division Southeast (MND-SE)*";
- "*New operational concepts and technological developments in the Allied context*".

Event photo: Scientific Seminar on "Consolidated national defence – fundamental operating concept for the Romanian Army 2021-2024"

As every year, the main objective of the event was to create a favourable environment for debates and exchange of views among participants concerned with security and defence, and to disseminate the results of scientific research, on which occasion the participants expressed their appreciation of the way the activity was organized and conducted.

Raluca STAN [*]

[*] ***Raluca STAN works at the Scientific Events Department of the CDSSS.***
E-mail: stan.raluca@unap.ro

WORKSHOP

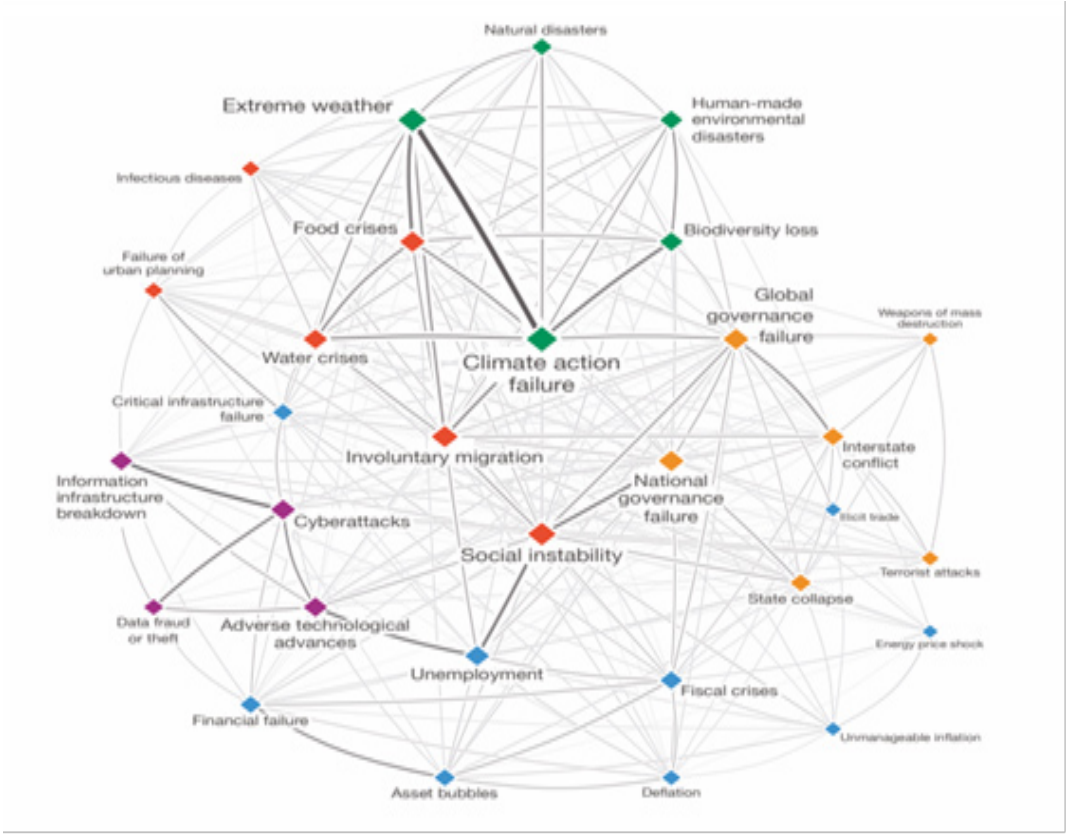
"The Impact of Climate Change on National Security (I)"

December 14th, 2022

Climate change is increasingly recognised as a "threat multiplier" by scientists, politicians and civil society around the world, and is a serious challenge today. While it is difficult to predict the consequences of this phenomenon, it is much easier to identify the steps needed to limit the consequences and slow it down as much as possible.

The workshop on "The impact of climate change on national security", organised by the CDSSS on December 14th, 2022, is the first stage of the project, planned for the period 2022-2024, according to the Sectoral Research and Development Plan of the Ministry of National Defence.

The scientific event aimed to identify issues related to the need for awareness of the climate change impact and ways to counter the effects of this phenomenon on national security against the backdrop of geopolitical and geo-economic changes, at a time of inflection in the way societies view the desired future. The unavoidable effects of climate change are increasingly visible, both nationally and internationally, whether in terms of intense heat waves, droughts destroying agricultural production, floods or threats to biodiversity from wildfires. The Russian Federation's war of aggression against Ukraine also threatens European security in an unprecedented way and exerts pressure on all sectors of the Union and its Member States, creating the need for them to become stronger, more resilient and more independent, particularly in the areas of defence, security, cyber security and critical infrastructure, but also energy, including energy efficiency.



Event photo: *Risk matrix according to the World Economic Forum 2020 report and connections between them*

The proposed theme created the scientific framework for substantive presentations and wide-ranging debates, the event bringing together expertise in the field from representatives of Defence, Public Order and National Security System structures, and from civil society, such as: Ministry of National Defence structures (Defence Staff, Land Forces Staff, Maritime Hydrographic Directorate, Air Component Command), Ministry of Internal Affairs (Police Academy), Ministry of Foreign Affairs (Euro-Atlantic Resilience Centre E-ARC), Ministry of Environment, Water and Forests (Directorate General for Impact Assessment, Pollution Control and Climate Change), National Meteorological Administration (Applied Meteorology), Ministry of Agriculture and Rural Development (Authority for the Administration of the National Anti-Hail and Rainfall Increase System). The activity was also shaped by the presence of foreign representatives with expertise in the field of climate change from institutions such as Defence Staff − France and University of Library Studies and Information Technologies − Bulgaria.

Event photo: *Workshop with the theme "The impact of climate change on national security"*

By the topics addressed, the scientific level of the debates, the participants and the results obtained, we can state that the scientific event organized by CDSSS was a success, providing both an academic framework for high quality debate and a real support to the educational process within the "Carol I" National University of Defence.

Otilia LEHACI [*]

[*] ***Otilia LEHACI works at the Scientific Events Department of the CDSSS.***
E-mail: lehaci.otilia@unap.ro

GUIDE FOR AUTHORS

We welcome those interested in publishing articles in the academic journal *Strategic Impact*, while subjecting their attention towards aspects to consider upon drafting their articles. **Starting with issue no. 1/2023, the journal shall be published in the English language only!**

MAIN SELECTION CRITERIA are the following:

- ✓ **Compliance with the thematic area of the journal – security and strategic studies** and the following topics: political-military topical aspects, trends and perspectives in security, defence, geopolitics and geostrategies, international relations, intelligence, information society, peace and war, conflict management, military strategy, cyber-security;
- ✓ **Originality** of the paper – own argumentation; novelty character – not priorly published;
- ✓ **Quality of the scientific content** – neutral, objective style, argumentation of statements and mentioning of all references used;
- ✓ **A relevant bibliography**, comprising recent and prestigious specialized works, including books, presented according to herein model;
- ✓ **English** language shall meet academic standards (British or American usage is accepted, but not a mixture of these).
- ✓ **Adequacy to the editorial standards adopted by the journal.**

EDITING NORMS

- ✓ **Article length** may vary between **6 and 12 pages** (25.000 - 50.000 characters), including bibliography, tables and figures, if any.
- ✓ **Page settings**: margins – 2 cm, A 4 format.
- ✓ The article shall be written in **Times New Roman font, size 12, one-line spacing.**
- ✓ The document shall be saved as Word (.doc/.docx). The name of the document shall contain the author's name.

ARTICLE STRUCTURE

- ✓ **Title** (centred, capital, bold characters, font 24).
- ✓ **A short presentation of the author**, comprising the following elements: given name, last name (the latter shall be written in capital letters, to avoid

confusion), main institutional affiliation and position held, military rank, academic title, scientific title (PhD title or PhD Candidate – domain and university), city and country of residence, e-mail address.

- ✓ A relevant **abstract**, not to exceed 150 words (italic characters)
- ✓ 6-8 relevant **keywords** (italic characters)
- ✓ **Introduction / preliminary considerations**
- ✓ **2 - 4 chapters** (numbered, starting with 1) (subchapters if applicable)
- ✓ **Conclusions**.
- ✓ **Tables / graphics / figures**, if they are useful for the argumentation, with reference made in the text. They shall be also sent in .jpeg /.png/.tiff format as well.

In the case of tables, please mention above "**Table no. X**: Title", while in the case of figures there shall be mentioned below (e.g. maps, etc.), "**Figure no. X:** Title" and the source, if applicable, shall be mentioned in a footnote.

REFERENCES

It is academic common knowledge that in the Abstract and Conclusions there shall not be inserted any references.

The article shall have references and bibliography, in the form seen below. Titles of works shall be mentioned in the language in which they were consulted, with transliteration in Latin alphabet if there is the case (e.g. in the case of Cyrillic, Arabic characters, etc.). Please provide English translation for all sources in other languages.

The article will comprise in-text citation and bibliography (in alphabetical order), according to The Chicago Manual of Style[1], as in examples below:

BOOK

Reference list entries (in alphabetical order)

Grazer, Brian, and Charles Fishman. 2015. A Curious Mind: The Secret to a Bigger Life. New York: Simon & Schuster.

Smith, Zadie. 2016. Swing Time. New York: Penguin Press.

In-text citation

(Grazer and Fishman 2015, 12)

(Smith 2016, 315–16)

[1] URL: https://www.chicagomanualofstyle.org/tools_citationguide/citation-guide-2.html

CHAPTER OF AN EDITED BOOK

In the reference list, include the page range for the chapter. In the text, cite specific pages.

Reference list entry

Thoreau, Henry David. 2016. "Walking." *In The Making of the American Essay*, edited by John D'Agata, 167–95. Minneapolis: Graywolf Press.

In-text citation

(Thoreau 2016, 177–78)

ARTICLE

In the reference list, include page range for the whole article. In the text, cite specific page numbers. For article consulted online, include a URL or the name of the database in the reference list entry. Many journal articles list a DOI (Digital Object Identifier). A DOI forms a permanent URL that begins https://doi.org/. This URL is preferable to the URL that appears in your browser's address bar.

Reference list entries (in alphabetical order)

Keng, Shao-Hsun, Chun-Hung Lin, and Peter F. Orazem. 2017. "Expanding College Access in Taiwan, 1978–2014: Effects on Graduate Quality and Income Inequality." *Journal of Human Capital* 11, no. 1 (Spring): 1–34. https://doi.org/10.1086/690235.

LaSalle, Peter. 2017. "Conundrum: A Story about Reading." *New England Review* 38 (1): 95–109. Project MUSE.

In-text citation

(Keng, Lin, and Orazem 2017, 9–10)

(LaSalle 2017, 95)

WEBSITE CONTENT

Reference list entries (in alphabetical order)

Bouman, Katie. 2016. "How to Take a Picture of a Black Hole." Filmed November 2016 at TEDxBeaconStreet, Brookline, MA. Video, 12:51. https://www.ted.com/talks/katie_bouman_what_does_a_black_hole_look_like

Google. 2017. "Privacy Policy." Privacy & Terms. Last modified April 17, 2017. https://www.google.com/policies/privacy/

Yale University. n.d. "About Yale: Yale Facts." Accessed May 1, 2017. https://www.yale.edu/about-yale/yale-facts

Citare în text

(Bouman 2016)

(Google 2017)

(Yale University, n.d.)

NEWS OR MAGAZINE ARTICLES

Articles from newspapers or news sites, magazines, blogs, and like are cited similarly. In the reference list, it can be helpful to repeat the year with sources that are cited also by month and day. If you consulted the article online, include a URL or the name of the databases.

Reference list entries (in alphabetical order)

Manjoo, Farhad. 2017. "Snap Makes a Bet on the Cultural Supremacy of the Camera." *New York Times*, March 8, 2017. https://www.nytimes.com/2017/03/08/technology/snap-makes-a-bet-on-the-cultural-supremacy-of-the-camera.html

Mead, Rebecca. 2017. "The Prophet of Dystopia." *New Yorker*, April 17, 2017.

Pai, Tanya. 2017. "The Squishy, Sugary History of Peeps." *Vox*, April 11, 2017. http://www.vox.com/culture/2017/4/11/15209084/peeps-easter

In-text citation

(Manjoo 2017)

(Mead 2017, 43)

(Pai 2017)

For more examples, please consult The Chicago Manual of Style.

SCIENTIFIC EVALUATION PROCESS is developed according to the principle *double blind peer review*, by university teaching staff and scientific researchers with expertise in the field of the article. The author's identity is not known by evaluators and the name of the evaluators is not made known to authors.

Authors are informed of the conclusions of the evaluation report, which represent the argument for accepting/rejecting an article.

Consequently to the evaluation, there are three possibilities:

a) the article is accepted for publication as such or with minor changes;

b) the article may be published if the author makes recommended improvements (of content or of linguistic nature);

c) the article is rejected.

Previous to scientific evaluation, articles are subject to an *antiplagiarism analysis*.

DEADLINES:

All authors will send their articles in English to the editor's e-mail address, **impactstrategic@unap.ro**.

We welcome articles all year round.

NOTA BENE:

Authors are not required any fees for publication and are not retributed.

By submitting their materials for evaluation and publication, the authors acknowledge that they have not published their works so far and that they possess full copyrights for them.

Parts derived from other publications should have proper references.

Authors bear full responsibility for the content of their works and for ***non-disclosure of classified information*** – according to respective law regulations.

Editors reserve the right to request authors or to make any changes considered necessary. Authors give their consent to possible changes of their articles, resulting from review processes, language corrections and other actions regarding editing of materials. The authors also give their consent to possible shortening of articles in case they exceed permitted volume.

Authors are fully responsible for their articles' content, according to the provisions of *Law no. 206/2004 regarding good conduct in scientific research, technological development and innovation*.

Failing to comply with these rules shall trigger article's rejection. Sending an article to the editor implies the author's agreement on all aspects mentioned above.

For more details on our publication, you can access our site, http://cssas.unap.ro/en/periodicals.htm or contact the editors at impactstrategic@unap.ro

"CAROL I" NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE

Layout editor: Gabriela CHIRCORIAN

The publication consists of 104 pages.

"Carol I" National Defence University Printing House
Şoseaua Panduri, nr. 68-72, sector 5, Bucureşti
E-mail: editura@unap.ro
Tel: 021/319.40.80/215

54/02.02.2023 C. 37/2023