

## THE IMPORTANCE OF MILITARY SCIENCES TO ENSURE NATIONAL SURVIVAL IN FUTURE CONFLICTS

*Captain (N) (r) Sorin TOPOR, Ph.D\**

*(Academy of Romanian Scientists, 3 Ilfov, 050044, Bucharest, Romania)*

**Abstract:** *The recognition of the field of military sciences, intelligence and national security as academic sciences is gaining more and more consistency for guaranteeing national security, not only by forming and strengthening the culture of national security, but by integrating scientific results from other recognized academic fields. Based on the results obtained, military technology manufacturers will identify new directions of development and optimize the allocation of resources for the implementation of emerging and disruptive techniques and components specific to the current period characterized by unprecedented geopolitical conflicts with influences on all levels of global economic development. The analysis of the particularities of this field of sciences and the presentation of specific limitations do not undermine their value but transform them into a strong vector of social and economic development, at the regional and national level, thereby strengthening the security and defense of the country and the alliances of which we are a part.*

*The paper is a critical analysis of the field of military science and its interaction with other fields of science, based on lessons learned from the conduct of the war in Ukraine. The formulated conclusions restore the role and place of military sciences in the panoply of academic disciplines and emphasize that the implementation of specific scientific results can contribute essentially to national survival in the context of establishing the directions of evolution of future wars.*

**Keywords:** *military science, academic disciplines, national security and defense, emerging and disruptive technologies.*

### **Introduction**

Normally, the concept of "military science" as an academic definition is not accepted, often citing the impossibility of formulating and testing hypotheses, theories, and laws that describe natural and social behaviors. Moreover, against the background of extensive discussions regarding non-compliance with the develop regulations and in the light of evidence of plagiarism by some authors, the idea is generalized that the results obtained through scientific research in the field of military sciences, intelligence and national security cannot be revised, they are not objective and are not reproducible.

As known, science is defined as an organized system of objective and verifiable knowledge acquired through observation, experimentation and progressive reasoning. This means that understanding and knowledge

---

\* National Institute for Research and Development in Informatics, ICI Bucharest/ Associate member of the Academy of Romanian Scientists, email: sorin.topor@ici.ro

increase as research continues and technologies advance. As the science of approaching military conflict cannot be denied by the purpose and effects that a war produces, we ask ourselves how this field can be defined observing that, in the period we are going through, in order to achieve victory and ensure the maintenance of the survival of a political-administrative system, there is a science that integrates the results of all recognized academic fields, in a mosaic of programs of history, foreign affairs, management and security, advanced technologies, other fields of natural, physical and social sciences.

The current Russian-Ukrainian war, as well as the other conflicts currently taking place, anywhere on the globe, represent testing laboratories of military technologies and not only, of asymmetric and hybrid operational algorithms, with an unprecedented development, from the results of which all countries learn. Through this specific knowledge, it is sought to predict how a system can defend itself under the conditions of a new type of war.

Generally, the development of knowledge in the fields of military science, intelligence and national security is a complex and continuous process that requires interdisciplinary approaches, considerable resources, integration of complex solutions and testing under conditions of small-time reserves, involves specialists, specific materials and environments appropriate, similarly to the development of any field of science. It is certain that without such an integrative approach of the recognized sciences no notable results can be achieved in contemporary military operations and no country's survival can be guaranteed in the sense of maintaining governance, autonomy and sovereignty over national goods and services.

We believe that the performance level of knowledge in the field of military science can be estimated by evaluating the following key aspects:

1. *Quality of information used:* Gathering and analyzing information about the enemy, terrain, and its resources are vital activities for structures engaged in conflict. They involve intelligence activities, obtaining scraps of information or relevant data by various means and techniques that are procedurally no different from those used in all known economic and social systems. Only the purpose and belonging to the intelligence services differ. The analysis and evaluation of this information outlines the picture of the current and prospective situation. During these activities, new technologies such as artificial intelligence (AI) and machine learning (ML) can be involved, which identify patterns and trends of evolution, activity identical to any modern management structure.

2. *Ways to integrate information:* The information obtained must be integrated into the planning and execution of military operations. This requires effective communication and collaboration between the structures of the armed forces involved, at the national level but also with international partners, if applicable. In the context of conducting a military operation,

operational information can only be made public, in part, after the war is over, for post-action analysis and the establishment of lessons learned. They are especially relevant in situations where an action has produced collateral effects well above the levels accepted by the conventions and international regulations.

3. *Technological innovation*: To gain the strategic advantage the development of military technology is essential in case of a war. This may include the development of new weapons, secure communication systems and technologies, advanced defense systems, other innovations that can change the combat dynamics.

4. *Continuous adaptation to changes in any field*: During a war, the situation of the operating environment can rapidly change due to a multitude of factors. The adaptability of the structures involved as well as the adaptation of plans and tactics to these changes are determining factors for the evolution in accordance with strategic goals. Moreover, in case of war, can change rapidly the situation on the ground, which requires a permanent adaptation and adjustment of the plans and tactics, the optimization of management cannot be achieved without a flexibility of thinking in action.

5. Another extremely important aspect to current conflicts concerns *the cyber security of systems*. In the digital age, the cyber security of communication networks and IT systems is essential to maintain the informational advantage and not only to ensure cyber defense against hybrid attacks.

6. Last but not least, the development of *knowledge to manage risks* in the conflicts is a permanent objective of any military strategy without which threats to own forces cannot be assessed, vulnerabilities and other potential dangers to all systems cannot be managed that form the structure of an actor, whether they are directly involved or that supports the cause of an actor directly involved.

Voelz<sup>1</sup> pointed out that the decline of the "military science" term is the result of the attempt to conceptualize and over-institutionalize officer training programs that emphasize the formalized study of military theory. He identifies as a factor undermining the art of war, the rapid pace of industrialization on firm scientific and technological bases, which are fundamental elements in the approach to doctrines and military planning and which determine the military power of a state. Thus, a reduction of the decision-making process to already formulated processes was achieved and not to the art of composing new formulas by mixing existing ones (a process

---

<sup>1</sup> Voelz, G. (2014), Is Military Science "Scientific"?, JFQ, 4th Quarter 2014, available at [https://www.researchgate.net/publication/329625323\\_Is\\_Military\\_Science\\_Scientific](https://www.researchgate.net/publication/329625323_Is_Military_Science_Scientific), accessed on 21.03.2024.

similar to science in any field, observable more often in the chemistry discipline). Thus, a distillation of the complexity of social dynamics into descriptive theories was obtained, applicable to scenarios limited to the planning and conduct of a military operation, hidden from the general audience. The content of the military sciences, even if it is more appropriate to the field of the social sciences, cannot be included and limited to it, especially in terms of estimating the hypothetical implications of all national systems in a war that must not take place. Therefore, the absence of controlled experiments, replicable by validating the theories obtained, but also of other determinations recognized by other academic environments, causes tensions regarding the integration of this science, specific to military professionals, among the recognized academic sciences. But we ask those who deny this field whether history has shown that there was even a single case where a war could be won without science.

We propose by studying the various aspects identified based on the lessons learned in the context of the war in Ukraine, to draw attention to the way of development of this field of sciences, with implications for determining the relationships and directions for maintaining national security and defense in a possible future war. Last but not least, the stimulation of interdisciplinary knowledge in fields of real and human disciplines will create a potential for complete transformation not only of military technologies but also of capabilities and practices in industry, with a considerable contribution to national social and economic development.

### **1. Details of the development of knowledge during the war in Ukraine**

I have chosen for analysis the war in Ukraine because it represents the conflict from the analysis of which anyone can observe the unprecedented rate of the adaptation of tactics and fighting techniques, as well as the steps of implementation of the latest technologies, of the modernization of equipment older or implementing new commercial technologies and equipment for military purposes. This war, which some theorists call war of attrition, produces an enormous amount of movement-counter-movement or action-counteraction functional relationships.

A first particularity of it is that both the Russian and Ukrainian military forces base, to a large extent, on the use of drones, manufactured for both military and commercial purposes. They are piloted by military, volunteers and civilians. Hundreds of drone systems are used in a mix of military, commercial, hobbyist etc., purposes for photography and video recording. At the combat zone, they are used in surveillance missions, gathering and correcting information in real time, for propaganda, for directing and coordinating the fire of artillery and other strikes, air and missile. Loaded with

explosives, drones can hit combat devices (trenches and critical infrastructure components) and moving or stationary vehicles (tanks, artillery pieces, naval ships, trucks etc.). To neutralize them, Russian forces use jamming systems, with emissions on the radio control signals of Ukrainian drones. To denial jamming, Ukrainian programmers change the operating frequencies of the drones. The scale and diversity of the use of these drones is enormous observable by the exaggerated consumption of equipment (about 10000 drones per month)<sup>2</sup>.

The most relevant conclusion regarding the importance of using drones in combat missions results from the naval war in the Black Sea. Thus, a state without a fleet, such as Ukraine, forced the Russian fleet to withdraw from its base in Sevastopol, Crimea, to the port of Novorossiysk, which is located far beyond the range of Ukrainian naval drones. Savitz and Courtney<sup>3</sup> observed that through the use of naval drones the Russian maritime power that had initially established dominance in the Black Sea was blocked. The scale of the destruction also benefited from Turkey's special support, by closing the Bosphorus Strait to military ships from outside the Black Sea nations (according to the Montreux convention). Thus, Russia was no longer able to strengthen its fleet to losses compensate.

In some situations, weather conditions affected the land mobility of force and logistics support, concentrating forces on practicable roads. These routes quickly became very congested. Thus, lines of Russian tanks and carriers became vulnerable to small and fast teams of armored hunters, equipped with drones and Javelin systems.

In the cyber security domain, a number of solutions have been developed and tested for attacking and protecting critical military and civilian infrastructures against cyber-attacks. The Russians created viruses to disrupt military communications and force Ukrainians to use commercial phones vulnerable to electronic warfare measures. Moreover, in the moments leading up to the invasion, Russia removed the Viasat satellite networks, cutting off Internet access for tens of thousands of Ukrainian citizens.

However, the cyber operations that followed were unprecedented, with Ukraine supported by civilian and military partners from the US, UK and other European countries. The large number of devices that could connect to the Internet offers a particular advantage in the realization of inter-human communication but also establishes a considerable number of cyber risks and

---

<sup>2</sup> Franke, U. (2023), Drones in Ukraine and beyond: Everything you need to know, European Council on Foreign Relations, available at <https://ecfr.eu/article/drones-in-ukraine-and-beyond-everything-you-need-to-know/>, accessed on 25.03.2024.

<sup>3</sup> Savitz, S. & Courtney, W. (2023), The Black Sea and the Changing Face of Naval Warfare, RAND, Objective Analysis. Effective Solutions, available at <https://www.rand.org/pubs/commentary/2023/10/the-black-sea-and-the-changing-face-of-naval-warfare.html>, accessed on 25.03.2024.

vulnerabilities that translate into data theft, cyber impersonation and access points for adversary entities. Cyber equipment, once compromised, can be used to compromise the entire network of connected systems, with broad implications for maintaining control over semi-autonomous weapons, potentially facilitating the execution of subversive, false-flag actions<sup>4</sup>. Thus, not only military technologies are affected, but all integrated cyber systems, through the manipulation of decision-making processes. Health and life insurance systems, systems that ensure societal comfort, energy systems, transportation and other cyber-physical systems integrated into cyber components of critical infrastructures may be affected.

In terms of decision-making processes, the leadership of military units was decentralized, with military structures being provided with information sets sufficient to carry out their mission and not to be identified by electronic surveillance systems. However, it is noted that civilian mobile telephone systems were left in operation, presumably to increase the amount of information at a given time. Any current mobile phone has photo/video transmission functions as well as geolocation. Certainly, vulnerabilities in commercial telephone systems have been exploited by electronic warfare units to intercept unsecured communications and launch disinformation and radio propaganda products. It was observed that, against orders, Russian soldiers and even their commanders provided sufficient information to the Ukrainian military, through the use of personal mobile phones, allowing them to geo-locate them and destroy by fire and combat action numerous combat systems, as well as to kill important military leaders. In addition, drone and mobile phone videos for propaganda purposes have brought viewers around the world closer to the real images of war, human injuries and deaths, the insecurity of combatants' positions etc., sometimes facilitating ambushes and encouraging desertions of Russian military.

As a product of military science, Russian specialists managed within a few months to identify solutions and build GPS jamming equipment to disrupt the accuracy of Ukrainian strikes with JDAM and Excalibur munitions, provided by the US and its allies. Initially, these weapons were considered to be protected against electronic attacks of the adversary. As a reaction measure, allied specialists managed to adapt the electronic protection systems of the systems and munitions made available to the Ukrainian armed forces so that they were functional again and hit targets with precision.

---

<sup>4</sup> Cameron, L. (2018), Internet of Things Meets the Military and Battlefield: Connecting Gear and Biometric Wearables for an IoMT and IoBT, IEEE Computer Society, available at <https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-ioimt-iobt> , accessed on 27.03.2024.

Another particular factor of this war is the use of satellites for real-time imagery, strike management and damage estimation<sup>5</sup>. Ukraine does not have its own satellites, at the beginning of the war the services were provided by the constellations of the Russian satellite system. But with the provision, as humanitarian support, of Starlink satellites by Elon Musk and American satellite services (HawkEye 360 and Maxar), as well as the services of the company's Satellogic (Argentina), ICEYE (Finland) and many others, Ukraine achieved a strategic advantage over Russia, with space becoming crucial to Ukrainian communications that provided access to high-speed Internet and secure communications to both the government and the public. On the other hand, the Russians managed to hack the technologies of the Starlink low-orbit satellites and threaten to shoot them down. Only the complexity of the situation (satellites belonging to SpaceX American company) stopped a physical attack. However, where possible, the Russians are implementing a number of electronic measures to disrupt their operation.

Within military management and beyond, working out how to manage, develop and protect space technology are topics that are receiving a lot of attention amid claims such as Russia's plans to put a nuclear anti-satellite system into space<sup>6</sup>. Moreover, the ambiguity of the situation of this war leads many theoreticians to propose a projection of the army as a regulatory force of complex causes, through which to adopt intervention strategies by combining the precision of weaponry with application methods based on various theories and doctrines.

It is becoming increasingly clear that against the background of the evolution of the systems and tactics specific to this war, new approaches to the conflict are needed, with dimensions that have overtaken the spatial ones, traditional land, air and naval military operations. Winston Churchill's prescient conclusion regarding the "Battle of the Beams"<sup>7</sup>, related to the conditions of the Second World War, takes increasingly sophisticated forms in ensuring the asymmetric advantage against the most advanced war technologies. Based on the concept of proxy warfare, more and more countries are adopting programs to develop weapons and security systems capable of demonstrating the ability to survive and fight in an increasingly contested and congested environment, thereby making it difficult for

---

<sup>5</sup> Wood, G. (2024), A Suspicious Pattern Alarming the Ukrainian Military, *The Atlantic*, available at <https://www.theatlantic.com/international/archive/2024/03/american-satellites-russia-ukraine-war/677775/>, accessed on 27.03.2024.

<sup>6</sup> Kimball D.G. (2024), U.S. Warns of New Russian ASAT Program, *Arms Control Association*, available at <https://www.armscontrol.org/act/2024-03/news/us-warns-new-russian-asat-program>, accessed on 25.03.2024.

<sup>7</sup> Hutton, R. (2021), 'Battle of the Beams': Germany's Invisible Secret Weapon that Could Have Devastated Britain, *Historynet*, available at <https://www.historynet.com/battle-of-the-beams-the-time-germany-devised-an-invisible-weapon-that-could-devastate-britain/>, accessed on 28.03.2024.

adversaries to continue occupying new territories and gaining new influence at the expense of allies and cooperation partners.

Therefore, not only the military learns from this war. Russian weapon systems have shown significant performance and the munitions provided to Ukraine have also shown vulnerabilities. The lessons learned from this conflict determine extensive changes and adaptations not only technological but also conceptual for all security systems of any state. The war in Ukraine proves that a military-industrial complex allows not only the development of military capabilities but also security capabilities within any technological approach. For example, according to reports, Russia's success in drone warfare is partly related to the density of electronic warfare systems it can deploy on the combat engagement front. A RUSI report<sup>8</sup> concluded that Russia is capable of deploying an electronic warfare system every 10 Km in defense-in-depth to support countermeasures against Ukrainian drones and take control of them, while obtaining the coordinates of the drone pilot's location, with an accuracy of up to one meter, sending these coordinates to the artillery units. These military applications involve AI/ML algorithms, which causes Western specialists to be extremely attentive to the development of operational techniques and skills.

In this war, many private and state companies are involved in the provision of emerging and disruptive technologies. Moreover, approaching war through a technological vision enables and motivates scientific research to the extent that the results can be replicated in a future conflict. Analysts have called this conflict “the first commercial space war, the first full-scale drone war, and the first AI war”<sup>9</sup>. It is predicted that this war will be won by the side that will be able to innovate more and more quickly. Ukraine would not have lasted this long without the support of using drones, without cloud services and cyber defense, without AI/ML and without satellites<sup>10</sup>. Numerous technology companies in the US, Europe and Asia provided high technology and cyber support to both actors, enabling and motivating fighters and other volunteers to find solutions to modernize older weapons systems. Amazon is known to have supplied Ukraine with digital data storage units for

---

<sup>8</sup> Watling, J. & Reynolds, N. (2023), Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine, RUSI, available at <https://www.rusi.org/explore-our-research/publications/special-resources/meatgrinder-russian-tactics-second-year-its-invasion-ukraine>, accessed on 28.03.2024.

<sup>9</sup> Franke, U. & Sodertrom, J. (2023), Star tech enterprise: Emerging technologies in Russia's war on Ukraine, European Council on Foreign Relations, European Power, available at <https://ecfr.eu/publication/star-tech-enterprise-emerging-technologies-in-russias-war-on-ukraine/>, accessed on 29.03.2024.

<sup>10</sup> Botezatu U.E. & Vevera V. (2023), Revolutionizing space security: The Laser Patroller Satellite – A technological marvel of modern warfare, in Buletin of „Carol I” National Defence University, No. 2/2023, available at <https://doi.org/10.53477/2284-9378-23-18>, accessed on 29.03.2024.



the transfer and storage of strategic information in the cloud. Google has extended the cyber protection of Ukrainian websites by offering free Project Shield software. CRDF Global has become a platform for the Cyber Defense Assistance Collaborative, an extensive network of US companies and organizations providing support to the Ukrainian government as well as other critical infrastructure entities.

## **2. Results and Discussions**

All these extremely brief analyses, reinforce the need to recognize the field of military science as an integrative field which, in the view of those presented, has exceeded the traditional sphere of responsibility of military education and scientific research related to the organization and development of war. Likely, the confusion of the dilemma of whether military science is a science is supported by formal planning and less analytically rigorous compared to other branches of science. But the rational criticism of the research results in the field of military sciences, which assumes a specific framework for war, requires the application of scientific methods in the study of destruction, losses and collateral effects in a short time and in a lack of relevant information.

Who undertakes the creation of such a laboratory, even a simulated one, just for the sake of observing scientific rigor? And in other fields of science there are unfounded assumptions and results that are eliminated over time through exercises, statistical analysis, and technological developments in that field. The demonstrative force is replaced by the number of examples. In fact, the field of military sciences most quickly eliminates those doctrinal elements based on the consolidation of the cult of expertise, on servility towards certain techniques, tools and traditional approaches. In the situation where the level of endowment with technique and weaponry does not allow their elimination, they are limited to a small number of examples. Clausewitz, the well-known Prussian general, military strategist and commander of the General War School in Berlin, drew attention to the dangers of superficial knowledge, due to the lack of time and misunderstanding of all the conditions of the production of an event with the mention that "the main evil... is not that the author never knew the respective events as the world, but that from this superficial, light-hearted treatment of history, a hundred wrong opinions and pseudo-theories arose afterwards..."<sup>11</sup>. Moreover, the complexity of knowledge and the interdisciplinarity of the field of military sciences fully support the lessons expressed by parables, by Malcom Gladwell in his book "Exceptional. The Success Story"<sup>12</sup>, namely that overconfidence is the

---

<sup>11</sup> Clausewitz, C. von, (2001), *Despre război*, (en. "On War"), Cartea a II-a, cap. 6, Antet Publishing House, Bucharest, p.70.

<sup>12</sup> Gladwell M., *Excepționalii, Povestea succesului*, (en. "Exceptional. The Success Story"), Publica Publishing House, Bucharest, 2009, ISBN 978-973-1931-14-2, available at

expert's disease. In the military, a commander can quickly create disasters if he does not perform a deep and rapid analysis of events, is not persistent in acquiring knowledge, and does not take advantage of the opportunities identified under all aspects of the technological approach to management.

Besides, there are also lessons learned about decisional abuses, which, by applying some skeptical methods, correct visions, theories and knowledge in order to limit and improve the techniques of cognition, in any field of sciences. Therefore, repositioning military science as an academic discipline of equal stature with the other established sciences, with the caveat that specific situations, knowledge, training and instruction are not sufficient to validate and accurately obtain results, will reduce the ambition of many decision makers to quickly achieve success functional, on the one hand, and will allow a sustainable and solid economic and social development of the systems, be they military.

In the context of the development of the Industry 4.0/5.0 concept, we appreciate that the interaction of military sciences with other sciences will be beneficial, especially through the perspective of the development and use of digital technologies, the Internet of Things (IoT), Operational Technology (OT), data analysis, cybernation process, AI/ ML, at least in the following directions:

1. Smart technology and connectivity: Improving, testing and validating the use of IoT/OT sensors and advanced communication networks for real-time monitoring and control of military and industrial equipment, as well as data collection and analysis;

2. Automation and robots: The use of robots and autonomous vehicles for surveillance tasks, transport of materials or even activities in contaminated or life-threatening environments, scenarios are somewhat similar to combat missions;

3. 3D Printing: Exploiting 3D printing technologies for the rapid and customized production of spare parts, equipment and systems can be a solution for both industries and the manufacture of weapons and ammunition;

4. Data analysis and AI/ML: In order to anticipate threats, risks evaluations and improve decisions, Big Data digital resources and AI/ML algorithms can contribute significantly to the development of the optimal use of resources of all kinds, with various destinations<sup>13</sup>;

---

<https://msbooks.club/books-motivatisisucces/1877-exceptionalii-povestea-succesului-de-malcolm-gladwell-pdf.html>, accessed on 30.03.2024.

<sup>13</sup> Stanciu A., Florian V., Ciuperca E.M. & Cîrnu C. E. (2020). A Review of Machine Learning Techniques for the Cybersecurity of Critical Infrastructures, International conference RCIC'20, Redefining Community in Intercultural Context, 9(1), 314–320, available at [https://www.afahc.ro/ro/rcic/2020/rcic'20/volum\\_2020/314-320%20-Stanciu.pdf](https://www.afahc.ro/ro/rcic/2020/rcic'20/volum_2020/314-320%20-Stanciu.pdf), accessed on 30.03.2024.

5. Augmented and virtual reality: These new technologies will make an essential contribution in the processes of training specialists and training staff, especially in the processes of training and training decision-makers for small formations, such as the heads of mobile industrial maintenance groups, group/platoon/company commanders etc.;

6. Cyber security: Developing and implementing cyber security solutions is a multidisciplinary challenge that goes beyond the training of an IT specialist. Good cyber security involves knowledge in the areas of network engineering, cryptography and data security, management, economics, standardization and law. Only through an integrated approach can the protection and resilience of critical infrastructures be achieved, be they economic, social or military<sup>14</sup>;

7. Autonomous weapon systems: Last but not least, the use of advanced technologies for the development and implementation of autonomous or semi-autonomous weapon systems, which can make decisions and act independently under certain conditions, represents a trend with great potential for the economic development of a countries. The formation of a defense industry that involves production facilities, networks and logistics systems, communication and financial systems, transport infrastructures and other specific elements can develop administrative regions and establish/consolidate relationships at the national and international level, within political and military alliances.

All these practices and technologies will also determine new challenges regarding the ethics and norms of the use of these systems, challenges that will have to be regulated by laws and other legal norms, in parallel with technological advances.

These observations emphasize the role and importance of the development of knowledge in the field of military sciences, intelligence and national security in the context of the trends of social and economic evolution of a country. It is noted that one of the strongest criticisms against their recognition as an academic discipline results from the special attention given to the publication of scientific results of military sciences which sometimes manifests a lack of transparency and excessive control of the way of obtaining and publishing the results, so as not to affect national security.

In the military, some research results may be classified or national security sensitive, and researchers must follow protocols and regulations

---

<sup>14</sup> Ciupercă E. M. & Vevera V. A. (2022), Solving and Managing Moral Dilemmas, From the Cyber Battle Field To The Future Of Mankind, In A. Lesenciuc. Proceedings of International Conference RCIC 22. Redefining Community in Intercultural Contexts, 10 (1), pp. 134-140, available at [https://www.afahc.ro/ro/rcic/2022/rcic'22/volum\\_2022/134-140%20Ciupercă-%20Vevera.pdf](https://www.afahc.ro/ro/rcic/2022/rcic'22/volum_2022/134-140%20Ciupercă-%20Vevera.pdf) accessed on 30.03.2024.

regarding the protection of classified information. In some situations, military researchers may be restricted in their travel to collect data and test research hypotheses, their collaboration with other researchers, and their ability to share information with similar structures in the other countries or with non-military entities. For the publication of the results, they must also consider the regulations imposed by the military institutions.

In addition, addressing topics of strategic and operational interest to military forces must be done with great care, with the publication of results requiring strong censorship to avoid revealing information that could affect military capabilities or operations. Even though the publication of results can play an important role in facilitating technology transfer to industry, they must consider legal aspects related to the protection of intellectual property and security, with most researchers being under the exclusive assignment contracts auspices.

Last but not least, the peer-review process is restricted or controlled to ensure that published information does not pose a risk to national security and defense. This process assumes that the assessment will be carried out by specialists with access to classified information or within the military professional communities. Therefore, the evaluation of researchers in the field of military sciences by statistical tools, such as the counting of cited papers and the confirmation of prestige by H-index, which confirm the relevance and quality of published papers, do not really reflect the quality of researchers in this field. Moreover, in the situation of accepting some works to be published in internationally indexed journals and conferences, and all the more appreciated under WOS scientometric analysis tools, without a control of the security structures, it would only make it available to an adversary potentially, for free, a series of information that would allow understanding the way of thinking and approaching a security issue. In this respect, academic transparency does not always benefit national security and defense. The effects of such transparency in hypothetical adversarial relationships erode defenses and can sometimes lead to vulnerabilities in the application of critical infrastructure resilience plans of national interest and serious delays in non-laboratory application conditions.

### **Conclusions**

Military, intelligence and national security sciences are similar to any recognized field of science, with particularities determined by the protection of the national strategic interest. Publishing research results in this area is a complex process that involves national security considerations, limited collaboration, and compliance with the military's strategic and operational objectives. For this it is important that researchers in the field are aware of all these aspects and act in accordance with the legal and regulatory provisions.

On the other hand, the evaluation of the specific results of this field cannot follow the same procedure as the similar processes of other sciences. Additional limitations and specialized audiences do not allow a military researcher to achieve academic visibility similar to researchers in other fields of science. In order to recognize the work done and the quality of the results, the military system must propose and implement another evaluation system.

Even so, it must be remembered that in the event of war, military science will integrate most new technologies and facilitate collaboration between military and civilian entities, between state and private companies, in order to strengthen national security. Ukraine would not have resisted the Russian attack without a collaboration and coordination of activities through a specific approach to military sciences. Without military science, Ukraine would not have used the cloud, the combat environment would have been analog, cyber technology would have been extremely limited, and the satellite services that ensured the connections between the structures of the armed forces, the government and the population would not have had the same effects.

The academic environment must understand that without military sciences, even the private companies that provide humanitarian support to Ukraine would not have faced the challenges of this type of geopolitical confrontation, with global economic effects.

On the other hand, the military must understand that all the emerging and disruptive technologies implemented in the structures of the armed forces cannot compensate for the lack of integration and coordination of economic objectives of national interest. The government of any country must concern itself with the realization of informal security assistance and recognize that the formation of national security culture and the training of citizens for defense is the key to the survival of any nation in future conflicts.



## BIBLIOGRAPHY

- BOTEZATU U.E. & Vevera V. (2023), *Revolutionizing space security: The Laser Patroller Satellite – A technological marvel of modern warfare*, in Buletin of „Carol I” National Defence University, No. 2/2023, available at <https://doi.org/10.53477/2284-9378-23-18>;
- CAMERON, L. (2018), *Internet of Things Meets the Military and Battlefield: Connecting Gear and Biometric Wearables for an IoMT and IoBT*, IEEE Computere Society, available at <https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt>;

- CIUPERCĂ E. M. & Vevera V. A. (2022), *Solving and Managing Moral Dilemmas, From the Cyber Battle Field To The Future Of Mankind*, In A. Lesenciuc. Proceedings of International Conference RCIC 22. Redefining Community in Intercultural Contexts, 10 (1), available at [https://www.afahc.ro/ro/rcic/2022/rcic'22/volum\\_2022/134-140%20Ciuperca%20Vevera.pdf](https://www.afahc.ro/ro/rcic/2022/rcic'22/volum_2022/134-140%20Ciuperca%20Vevera.pdf);
- CLAUSEWITZ, C. von, (2001), *Despre război*, (en. "On War"), Cartea a II-a, cap. 6, Antet Publishing House, Bucharest;
- FRANKE, U. (2023), *Drones in Ukraine and beyond: Everything you need to know*, European Council on Foreign Relations, available at <https://ecfr.eu/article/drones-in-ukraine-and-beyond-everything-you-need-to-know/>;
- FRANKE, U. & Soderstrom, J. (2023), *Star tech enterprise: Emerging technologies in Russia's war on Ukraine*, European Council on Foreign Relations, European Power, available at <https://ecfr.eu/publication/star-tech-enterprise-emerging-technologies-in-russias-war-on-ukraine/>;
- GLADWELL M., *Exceptionalii, Povestea succesului*, (en. "Exceptional. The Success Story"), Publica Publishing House, Bucharest, 2009, ISBN 978-973-1931-14-2, available at <https://msbooks.club/books-motivatisisucces/1877-exceptionalii-povestea-succesului-de-malcolm-gladwell-pdf.html>;
- HUTTON, R. (2021), *'Battle of the Beams': Germany's Invisible Secret Weapon that Could Have Devastated Britain*, Historynet, available at <https://www.historynet.com/battle-of-the-beams-the-time-germany-devised-an-invisible-weapon-that-could-devastate-britain/>;
- KIMBALL D.G. (2024), *U.S. Warns of New Russian ASAT Program*, Arms Control Association, available at <https://www.armscontrol.org/act/2024-03/news/us-warns-new-russian-asat-program>;
- SAVITZ, S. & Courtney, W. (2023), *The Black Sea and the Changing Face of Naval Warfare*, RAND, Objective Analysis. Effective Solutions, available at <https://www.rand.org/pubs/commentary/2023/10/the-black-sea-and-the-changing-face-of-naval-warfare.html>;
- STANCIU A., Florian V., Ciuperca E.M. & Cîrnu C. E. (2020). *A Review of Machine Learning Techniques for the Cybersecurity of Critical Infrastructures*, International conference RCIC'20, Redefining Community in Intercultural Context, 9(1), 314–320, available at [https://www.afahc.ro/ro/rcic/2020/rcic'20/volum\\_2020/314-320%20Stanciu.pdf](https://www.afahc.ro/ro/rcic/2020/rcic'20/volum_2020/314-320%20Stanciu.pdf);
- VOELZ, G. (2014), *Is Military Science "Scientific"?*, JFQ, 4th Quarter 2014, available at [https://www.researchgate.net/publication/329625323\\_Is\\_Military\\_Science\\_Scientific](https://www.researchgate.net/publication/329625323_Is_Military_Science_Scientific);
- WATLING, J. & Reynolds, N. (2023), *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine*, RUSI, available at

<https://www.rusi.org/explore-our-research/publications/special-resources/meatgrinder-russian-tactics-second-year-its-invasion-ukraine>;  
WOOD, G. (2024), *A Suspicious Pattern Alarming the Ukrainian Military*,  
The Atlantic, available at <https://www.theatlantic.com/international/archive/2024/03/american-satellites-russia-ukraine-war/677775/>;

