Hungarian Defence Review

SPECIAL ISSUE 2025,
VOL. 153, NR. 1

Issued by the HDF Command
Semi-annual publication

EDITORIAL STAFF

*The MoD Zrínyi Geoinformation and Recruitment
Support Public Benefit Non-profit Ltd.
– Zrínyi Publishing House
Editorial Board of Scientific Publications takes part
in publishing and distributing the journal.*

Responsible manager: General Manager Gábor KULCSÁR
Director of the Zrínyi Publishing House: Ferenc HAJDÚ PhD
Editor of the Special Issue: Orsolya Andrea BEDE
Proofreader: Boldizsár ESZES
Head of Editorial Office: Andrea SCHUBERT EISRICHNÉ
Head of Production: István GRÓF
Layout editor: Kitti PETREZSELYEM

Contacts:
E-mail: hdr@hmzrinyi.hu
Address: H-1024 Budapest, Szilágyi Erzsébet fasor 7–9.

The entire content of the *Hungarian Defence Review*
is accessible on https://hungariandefencereview.hu/

Printed by: MoD Zrínyi Non-profit Ltd.,
Creative Designing and Printing Department
Director of the Creative Designing and Printing Department:
Zoltán PÁSZTOR

HU ISSN 2060-1506

The *Hungarian Defence Review* is recognised by
the Hungarian Academy of Sciences as a category 'A'
benchmark publication.

The papers published by the *Hungarian Defence Review*
are reviewed and edited.

The *Hungarian Defence Review* is a member of
the European Military Press Association (EMPA).

FOR THE HOMELAND

HUNGARIAN DEFENCE FORCES

ZRÍNYI KIADÓ

Hungarian Defence Review

SPECIAL ISSUE 2025,
VOL. 153, NR. 1

CONTENTS

FORCE DEVELOPMENT

INNOVATION METHODOLOGIES FOR DEFENCE CHALLENGES

AFRICA AND ASIA

Zoltán Gábor Bárány, Péter Á. Kiss, Patrik György Szalkai

THE TRANSFORMATION OF THE HUNGARIAN DEFENCE FORCES

DOI: 10.35926/HDR.2025.1.1

ABSTRACT: *With the end of the Cold War, Hungary, like most European nations, allowed its considerable military capability to decline. As international crises followed each other in the early 21st century, the country's leadership realised that Europe's security situation was deteriorating and a credible deterrent force was needed to protect national borders and sovereignty. The Hungarian Defence Forces embarked on an ambitious transformation program in 2017, the two pillars of which are the modernisation of the entire defence sector and the creation of armed forces superior to all possible opponents. The paper provides a brief overview of the HDF transformation process that has taken place so far.*

KEYWORDS: *armed forces transformation, defence sector modernisation, security environment, Hungarian Defence Forces*

ABOUT THE AUTHORS:

- *Colonel Zoltán Gábor Bárány is an armoured corps officer. He is the commander of the Hungarian Defence Forces Transformation Command. (ORCID: 0009–0000–7311–500X; MTMT: 10098744)*
- *Dr Péter Á. Kiss is a senior civilian researcher at the Hungarian Defence Forces Transformation Command, Scientific Research Centre. (ORCID 0000-0002-0662-5381; MTMT: 10027615)*
- *Patrik György Szalkai is a civilian researcher at the Hungarian Defence Forces Transformation Command, Scientific Research Centre. (ORCID: 0000-0001-8004-3083; MTMT: 10088547)*

POST-COLD WAR COMPLACENCY

Before discussing the transformation of the Hungarian Defence Forces, we have to start with a few thoughts about what and where we are transforming from. At the end of the Cold War, Hungary had large, conscription-based armed forces. The number of service personnel comprised nearly 100,000 men on active duty as well as over 200,000 reservists to man 1,500 tanks, 2,000 armoured vehicles, and 1,100 artillery pieces. The Air Force had nearly 200 aircraft of various types.[1]

With the end of the Cold War, Hungary, like most European nations, allowed this considerable military capability to decline. Besides Hungary, the NATO alliance also saw a long period of peace, interspersed with small-scale expeditionary operations. We reduced the size of the armed forces, suspended conscription, gave up most of our heavy equipment,

[1] The Military Balance 1991, 88–89.

and saw no need to replace those assets that were withdrawn from service. By 2014, personnel and equipment were reduced by an order of magnitude, to just over 20,000 active strength and a handful of reservists, a few hundred armoured vehicles and less than 50 aircraft of all types.[2]

Then, the international crises of the last 10 years or so have made us realise that Europe's security situation is not nearly as stable as we thought, and a credible deterrent force is still needed to protect national borders and sovereignty. The protracted Russo-Ukrainian War is a warning that international borders are not inviolable and that the enormous destruction of a conventional war is still possible in Europe today. The continuous migration pressure since 2015 makes it clear that military assistance to the civil power may be necessary in times of peace. Taking these warning signs seriously, Hungary broke with the post-Cold War complacency, adopted more national security-centred policies, and took decisive steps to strengthen its defence posture.

DECISION AND MILESTONES OF TRANSFORMATION

We realised that the security environment was rapidly changing. The Russo-Ukrainian War showed us that there was an increased emphasis on military innovation and the adaptation of new capabilities, enabled by emerging and disruptive technologies. We had to reassess some national force development priorities and timelines to adjust to these new challenges.

We also realised that the Defence Forces have to increase the speed of adaptation to changes because the rapid evolution of technology outpaces military capability development, and we could maintain our flexibility and technological edge only through new, alternative, and innovative methods and a thorough change in culture. While we keep our national capability targets in sight, we are also putting an increased emphasis on harmonising and synchronising our efforts with Allied guidelines and concepts. To enable rapid adaptation to the ever-changing security environment, we decided to turn the HDF into a learning organisation and institutionalise transformation. By transformation, I mean a continuous, self-reinforcing process to prepare the HDF for the challenges of the future. It is more than just modernisation because it involves procedures, concepts, doctrines, and the general mindset of military professionals. These all need to change according to a common vision towards a shared goal.

So, what have been the milestones of the HDF's transformation so far?

Modernising and transforming the armed forces must be accompanied by a conceptual development at the level of political strategy, which provides appropriate foundations for the legal framework for the implementation of force development. In 2017, once the political leadership made its decision known, we embarked on a fast-paced, large-scale force development program, the Zrínyi 2026 Defence and Military Development Program, based on a thorough conceptual overhaul. The program's goal was to turn the HDF into a dominant military force in the region.[3] The Zrínyi 2026 Program's implementation was followed by the publication of two strategic documents.

[2] The Military Balance 2014, 106–107.

[3] Government of Hungary 2017; Nagy 2022.

In 2020, we published a new National Security Strategy that identified all the new risks and changes in the security environment and contemplated putting Hungary's defences on a new footing.[4] A year later, the National Military Strategy was published. This document defines ends, ways, and means to transform the Hungarian Defence Forces into a modern, sustainable, flexible, and effective force with a balanced structure, with high combat effectiveness, capable of being deployed in a wide range of crisis situations. It also contains – in a rather unorthodox manner – a description of the HDF we want to build. That force architecture is still valid today. We planned a three-brigade concept for the ground forces, with combat, combat support, and combat service support capabilities being developed gradually as resources became available. In this context, a heavy, a medium, and a special-purpose (light) brigade have been established. Subsequently, the plan was amended with the addition of a fourth brigade. With regard to combat support capabilities, significant improvements, mainly in terms of quality, are being made in the fields of intelligence and information technologies, engineering, chemical defence, and reconnaissance. Also, the new transformation system was detailed in this document.[5]

This is an exciting time to be in the top leadership of the armed forces, but it is also a difficult one because we are facing many challenges. We must prepare to fight the wars of the future without actually knowing what war will be like five, ten, or fifteen years from now.[6] Our materiel and human resources are limited, so we need to acquire mature and tested systems with plenty of evolutionary potential, and we need to find the equipment and procedures that will provide the best possible protection to our troops during operations.

As I mentioned, transformation has a dedicated organisation in the HDF.[7] It is a capability that every modern military needs. The HDF had recognised the importance of national transformation efforts earlier, so there were organisations that worked in the field of transformation, but such an organisation that could integrate the efforts at the system level did not exist. The changing security environment (with the Russian aggression in Ukraine and the increasing importance of new and disruptive technologies) reinforced the need for such institutions, and eventually, new organisations have been created. First, the Modernisation Institute and soon after, the Transformation Command were established. The former was responsible for the material development of the forces, while the latter for the non-material development. Both organisations have gone through several changes since, but the premise holds. We need and use these two functions every day.

Lessons of the Russo-Ukrainian War

Earlier, I mentioned in passing that preparing to fight the wars of the future is a challenge because we do not know what those wars will be like. The Russo-Ukrainian War, going on for almost three years now, is a kind of transition between the past and the future, but it does provide some clues. Both sides are using a lot of equipment that was put into the system 50 or 60 years ago. However, in addition to this, prototypes of the devices of the future also appear: a Starlink communication system, a fire-control system controlled by artificial intelligence, and air, land, and sea drones. Here are some lessons that we have discerned so far:

[4] Government of Hungary 2020.

[5] Government of Hungary 2021.

[6] Williams – Brawley 2025; Rajagopalan – Patil 2024; Rickli – Mantellassi 2024.

[7] Ruszin-Szendi 2023.

- Drones can be used en masse in the air, on land, or at sea since they are cheap and easy to obtain. It is almost impossible to hide from them, and even if they are identified in time, it is difficult to defend against them. This means that fundamental changes are necessary in air, land, and sea tactics.[8]
- There has been speculation about the demise of the tank. Certainly, both sides have lost thousands of armoured vehicles to drones and anti-tank missiles. But I am certain that the battles of the future will still require highly mobile, armour-protected firepower. Further experimentation and experience will determine whether it will be a manned or remote-controlled system.[9]
- A multi-layered air defence system that covers not only the battlespace but also our own and the enemy's rear areas in depth is capable of seriously constraining the enemy's air activities. However, fast and highly accurate missiles and glide bombs launched from a stand-off distance can get through most air defence systems. Defence against drones requires a different approach: close air defence, kinetic, and non-kinetic systems are needed. Weapons and equipment alone are not sufficient: innovative tactics, techniques, and procedures are also needed.[10]
- To maintain and increase the survivability and operational manoeuvrability of troops, individual and collective nuclear, biological, and chemical defence, technical combat support capabilities to support the movement of own forces and to impede the movement of the opposing side, as well as technical capabilities to support infrastructure and fortification construction will be developed.[11]
- We are also relearning a lesson from previous conflicts: the armed forces must be tailored to the war they are to fight. Small, highly trained, well-equipped professional formations are all very well in an expeditionary setting, but in a high-intensity war, against a strong and determined enemy, they are attrited in the first battles, unless they are supported by a large mass army.[12]

Additionally, a very important lesson is that in a high-intensity war, an enormous amount of materiel is needed. Vehicles and equipment are destroyed or worn out, and fighting enemy forces requires a staggering amount of ammunition. We must therefore rethink our norms for reserving stocks and make arrangements now to ensure a timely and uninterrupted supply of materiel, partly through the further expansion of our military industry and partly from reliable foreign resources.

NATO REQUIREMENTS AND NATIONAL GOALS

With our NATO membership, Hungary's security has increased significantly. We are now part of an extended zone of stability and security in Europe that guarantees a measure of protection against both old and new challenges. Our full membership gives us the opportunity to effectively represent and promote our national interests. At the same time, we can participate in shaping the Alliance's common defence strategy, objectives, and tasks in the planning and coordination processes that express its substance, and in shaping NATO's

[8] Franke 2024.

[9] Gardner 2022; Wolf 2024.

[10] Stoll et al. 2024; Balmforth 2023; Stalder – Patterson 2024.

[11] Vasyliuk 2024; Voitenko – Chaly 2024.

[12] Michta 2023; Martin 2024.

future. However, NATO membership not only increases our security but at the same time, it also imposes obligations on the HDF beyond the defence of the country. Our participation in international missions in Kosovo, Bosnia and Herzegovina, and Cyprus, as well as our contribution to the air defence of Slovakia and Slovenia, requires considerable resources, but it signals to our international partners that Hungary and the Hungarian Defence Forces are not freeloaders but active and reliable allies.[13]

Nationally, our goal is to build and maintain armed forces that are able to independently carry out the tasks outlined in the Fundamental Law of Hungary. They must be superior to all possible opponents, primarily by relying on their highly trained human resources, through technical improvements, and maintaining their superiority through continuous transformation. Capability development is carried out across the entire spectrum of capability areas, supported by continuous analysis and assessment of changes in the strategic environment, experience gained from the conduct of operations and exercises, defence research, operational and technological innovation, and concept and doctrine development.

The focus of the capability development is on the steady improvement of the combat, combat support, and combat service capabilities of the Hungarian Defence Forces, which increases the readiness, survivability, and operational effectiveness of the individual soldiers, as well as that of the HDF's combat formations by using the results of modern technology and innovation. Therefore, the directions for the development of indigenous defence industrial capabilities also cover technological capabilities that will define future warfare, such as information technology and cyber defence, simulation, virtual and augmented reality, artificial intelligence, quantum computing, robotics, unmanned systems, non-lethal weapons, energy storage and alternative energy sources, nanotechnology, materials technologies, and biotechnology.

Without the development of the defence industry, the development goal of transforming the Hungarian Defence Forces into a modern and capable military force cannot be fully achieved. Force development creates opportunities for defence-industrial cooperation, which, through technology transfer and the establishment of manufacturing capacities, creates the possibility for the transformation of the defence industry. The development of the Hungarian defence industry is essential for the long-term sustainability of successful force development.

MEETING THE CHALLENGES OF THE FUTURE

The successes of these past years, as well as these recently learned lessons, will be necessary if we look at the expected challenges of the future. If we look around the world, potential conflicts and intensifying competition are everywhere: China, Africa, the Middle East, and the Arctic. It is true that these areas are far from our borders, but since 9/11 and its aftermath, we have learned that distance does not mean that distant problems do not affect us.

In this intensifying future competition, securing resources will be even more important than today. Who owns the energy sources, raw materials, production capacities, and drinking water will fundamentally determine a country's position and opportunities. In addition to material assets, the value of expertise will also increase. Countries that cannot exploit their own resources due to a lack of expertise will fall behind.

[13] Böröndi 2024; Böröndi – Gazdag 2024; Consulate General of Hungary in Los Angeles [no year].

Of course, this changing and challenging world also affects NATO. As a result of the Russo-Ukrainian War, the organisation will return to its original role, and its central task will once again be the defence of Europe. This, in turn, will require a greater expenditure than ever before. We can already see that spending 2 percent of GDP on defence is not sufficient, and many states have already set much higher goals.[14]

The warfare of the future will require greater financial resources than ever before, but not necessarily greater sacrifices than ever before. Innovation will help us in this. If we are able to always stay one step ahead of our rivals, we can avoid suffering such losses as we have seen in the war in Ukraine. To do this, we need to excel in artificial intelligence and drone swarms. We need to prepare for capabilities that are already known today, such as firearms with a larger calibre and penetrating power or artillery that can fire on the move. And if we look further afield, we must start thinking today about the challenges posed and opportunities offered by nanotechnology and space capabilities. To prepare for all these challenges, Hungarian simulation and wargaming skills, which are developing at a rapid pace today, are essential.

One thing we are relearning during the force modernisation process is that it must be a continuous process. We cannot sit back after a year, two or three years, satisfied that we are done. We are not done.[15] The war in Ukraine and other current conflicts have generated the need for technological changes in the Hungarian Defence Forces. New equipment and new systems appear, presenting new challenges and necessitating organisational changes. It is obvious today that emerging and disruptive technologies will continue to pose a great challenge to global security and the security of Hungary. Periodically, we must return to projects that were already completed to see whether they need to be revised, regularly inspect equipment already in the inventory to see if it needs another round of modernisation, and constantly evaluate doctrines and training to see if they have to be brought up to date in line with new developments.

BIBLIOGRAPHY

- Balmforth, Tom: *Ukraine builds layered air defences as Russia ramps up strikes*. Reuters, 20 June 2023. https://www.reuters.com/world/europe/ukraine-builds-layered-air-defences-russia-ramps-up-strikes-2023-06-20/ (Accessed: 15/01/2024).
- Böröndi, Gábor: *Az európai védelmi architektúra jövője (The future of European defence architecture)*. Honvédségi Szemle, Vol. 152, No. 2 (2024), 3–6. https://kiadvany.magyarhonvedseg.hu/index.php/honvszemle/issue/view/146/147 (Accessed: 15/01/2024).
- Böröndi, Gábor – Gazdag, Erika: *Road to Hungary's EU Presidency: a Snapshot on the European Security*. Hadtudomány, Vol. 34, No. 1 (2024), 3–11.
- Consulate General of Hungary in Los Angeles: *Hungary and the World*. [no year]. https://losangeles.mfa.gov.hu/eng/page/hungary-and-the-world (Accessed: 15/01/2024).
- Fix, Liana – Kapp, Caroline (2024): *As NATO Countries Reach Spending Milestone, Is 2 Percent Enough?* Council on Foreign Relations, 28 June 2024. https://www.cfr.org/expert-brief/nato-countries-reach-spending-milestone-2-percent-enough (Accessed: 15/01/2024).

[14] Hawkins 2024; Fix – Kapp 2024.

[15] Rainey 2024; Kuzma 2022.

- Franke, Ulrike: *Drones in Ukraine: Four lessons for the West*. European Council of Foreign Relations, 10 January 2024. https://ecfr.eu/article/drones-in-ukraine-four-lessons-for-the-west/ (Accessed: 15/01/2024).
- Gardner, Frank: *Ukraine war: Is the tank doomed?* BBC, 7 July 2022. https://www.bbc.com/news/uk-61967180 (Accessed: 15/01/2024).
- Government of Hungary: *A Kormány 1298/2017. (VI. 2.) Korm. határozata a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program megvalósításáról (Government resolution 1298/2017. (02/06) on the execution of the Zrínyi 2026 Defence and Military Development Program).* 2017. https://magyarkozlony.hu/dokumentumok/1cb5b97a816d3757b350ef71bc589d931c1ec4d2/megtekintes (Accessed: 15/01/2024).
- Government of Hungary: *1163/2020. (IV. 2.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról (Government resolution 1163/2020 (21/04) on Hungary's National Security Strategy)*, 2020. https://honvedelem.hu/hirek/government-resolution-1163-2020-21st-april.html (Accessed: 15/01/2024).
- Government of Hungary: *1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról (Government Resolution 1393/2021 (24/06) on the National Military Strategy of Hungary)*, 2021. https://defence.hu/news/national-military-strategy-of-hungary.html (Accessed: 15/01/2024).
- Hawkins, Derek: *See which NATO countries spend less than 2 percent of their GDP on defense*. The Washington Post, 8 July 2024. https://www.washingtonpost.com/politics/2024/02/12/nato-countries-defense-spending-gdp-trump/ (Accessed: 15/01/2024).
- Colonel Kuzma, Gregory: *A Culture of Modernization is a mindset, not a buzz phrase*. Air Force, 13 January 2022. https://www.af.mil/News/Commentaries/Display/Article/2899139/a-culture-of-modernization-is-a-mindset-not-a-buzz-phrase/ (Accessed: 15/01/2024).
- Martin, Tim: *With an eye on Ukraine, head of British Army says 'mass is still indispensable'*. Breaking Defense, 27 June 2023. https://breakingdefense.com/2023/06/with-an-eye-on-ukraine-head-of-british-army-says-mass-is-still-indispensable/ (Accessed: 15/01/2024).
- Michta, Andrew A.: *Mass still matters: What the US military should learn from Ukraine*. New Atlanticist, 3 October 2023. https://www.atlanticcouncil.org/blogs/new-atlanticist/mass-still-matters-what-the-us-military-should-learn-from-ukraine/ (Accessed: 15/01/2024).
- Nagy, Dávid: *Development of the Hungarian Defence Forces since 1989*. Danube Institute, 2022. https://danubeinstitute.hu/en/research/development-of-the-hungarian-defence-forces-since-1989 (Accessed: 15/01/2024).
- General Rainey, James E.: *Continuous Transformation*. Military Review, No. 5 (2024), https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/September-October-2024/Continuous-Transformation/Continuous-Transformation-UA.pdf (Accessed: 15/01/2024).
- Rajagopalan, Rajeswari Pillai – Patil, Sameer: *Future Warfare and Critical Technologies: Evolving Tactics and Strategies*. Observer Research Foundation, 12 February 2024. https://www.orfonline.org/research/future-warfare-and-critical-technologies-evolving-tactics-and-strategies (Accessed: 15/01/2024).
- Rickli, Jean-Marc – Mantellassi, Federico: *The War in Ukraine: Reality Check for Emerging Technologies and the Future of Warfare*. Geneva Centre for Security Policy, 5 April 2024. https://www.gcsp.ch/publications/war-ukraine-reality-check-emerging-technologies-and-future-warfare (Accessed: 15/01/2024).
- Lieutenant General Ruszin-Szendi, Romulusz: *The Transformation of the Hungarian Defence Forces*. European Security & Defence, 26 May 2023. https://euro-sd.com/2023/05/articles/31346/the-transformation-of-the-hungarian-defence-forces/ (Accessed: 15/01/2024).

- Stalder, Keith – Patterson, Dean: *Reevaluating Modern Warfare: Lessons From Ukraine's Air Defense Strategies*. The Defense Post, 5 July 2024. https://thedefensepost.com/2024/07/05/ukraine-air-defense-strategies/ (Accessed: 15/01/2024).
- Stoll, Hunter – Hoehn, John – Courtney, William: *Air Defense Shapes Warfighting in Ukraine*. RAND, 22 February 2024. https://www.rand.org/pubs/commentary/2024/02/air-defense-shapes-warfighting-in-ukraine.html (Accessed: 15/01/2024).
- *The Military Balance 1991–1992*. International Institute for Strategic Studies, London, 1991.
- *The Military Balance 2014*. International Institute for Strategic Studies, London, 2014.
- Vasyliuk, Oleksiy: *Military fortifications in Ukraine – what comes next?* Ukraine War Environmental Consequences Work Group, 29 January 2024. https://uwecworkgroup.info/military-fortifications-in-ukraine-what-comes-next/ (Accessed: 15/01/2024).
- Voitenko, Anna – Chalyi, Sergiy: *Ukrainian soldiers, engineers toil round the clock to build defences*. Reuters, 4 April 2024. https://www.reuters.com/world/europe/ukrainian-soldiers-engineers-toil-round-clock-build-defences-2024-04-04/ (Accessed: 15/01/2024).
- Williams, Sarah – Brawley, Simon: *War and the future of war*. UK Parliament, 7 January 2025. https://post.parliament.uk/war-and-the-future-of-war/ (Accessed: 15/01/2024).
- Wolf, Fabrice: *Is the end of the battle tank in sight in the conflict in Ukraine?* Meta-defense.fr, 25 April 2024. https://meta-defense.fr/en/2024/04/25/late-battle-tank-in-ukraine/ (Accessed: 15/01/2024).

Dr Ferenc Hajdú, PhD

A SUCCESSFUL DEFENCE INNOVATION ECOSYSTEM

To Mark the Work of Colonel József Jáky, Ministerial Commissioner for Air Defence Radar Development

DOI: 10.35926/HDR.2025.1.2

ABSTRACT: *The lessons drawn so far from the Russo-Ukrainian War have shown that the failures of set objectives can be traced back not only to the errors of operational planning but also to shortcomings in the deployability of military equipment in given situations. Change is constant. The quality of (operational or military engineering) responses to the continuously changing situation is a function of the status of the defence innovation ecosystem. Economists, engineers, and doctors are looking to define the concept of innovation differently, based on the ecosystem surrounding them. The defence innovation ecosystem rests on three pillars: the current state of military science, the capabilities of the defence industry, and the defence requirements. Besides these three pillars, the defence innovation ecosystem's quality is determined by a network of connections among several other elements. What are the elements that need to be operated in the interest of a successful development? What are the connections among these elements? Can one give an exact description of all elements and connections of a defence innovation ecosystem, or does it have some general laws? This study aims to seek the elements of a defence innovation ecosystem required for fighting a successful war through the examination of a successful military technology research and development program: the Hungarian radar developments in the 1940s.*

KEYWORDS: *defence innovation ecosystem, research and development, radar development*

ABOUT THE AUTHOR:

Dr Ferenc Hajdú is a lecturer at Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering, at the Doctoral School of Military Sciences and the Doctoral School of Military Engineering at the Ludovika University of Public Service, Budapest (ORCID: 0000-0003-0449-7678; MTMT: 10002977).

ACKNOWLEDGMENTS

My thanks go to my friends Gyula Sárhidai and András Hatala, who helped me greatly in collecting the sources.

INTRODUCTION

The development of air defence radars during the Second World War was doubtlessly one of the most successful stories of research and development in Hungarian military technology. While researching the history of military technology, I examined the elements of the defence innovation ecosystem of the age, their connections, functioning, and the role of the talents who played a key part in development. My goal is to present the laws of cooperation among the scientific, industrial, military engineering, and operational elements necessary for the successful development of military hardware. In my account, I will lay emphasis on those engineering and operational requirements that triggered scientific and industrial responses during the "story".

HISTORICAL BACKGROUND TO THE DEFENCE INNOVATION ECOSYSTEM

Defence innovation is not a creation of the 21st century, being itself the product of an evolving process. The continuous development of ever-newer offensive and defensive assets and procedures has occurred throughout human history. The evolution of the armed forces has produced organizations and a network of connections needed for their development everywhere. Military technology research and development is not identical with defence innovation, although it forms an important part of it. Defence innovation is an unfolding process in a rapidly changing security environment, being conveniently organized by innovation management. In the overwhelming majority of cases, this process of innovation involves more than one player. Rather, it is the interaction of a complex network of partnerships and elements, which we call the innovation ecosystem. This interaction takes place among the three pillars of the defence innovation ecosystem (Triple Helix model[1]) and the elements connected with them.

Military Engineering Background to Radar Development

The lessons learned in the Battle of Britain showed that modern-day air defence cannot conceivably work without the use of radars. The Kingdom of Hungary expressed to Germany its interest in purchasing such equipment, but the Germans said no, as long as Hungary was unable to offset such a deal through the delivery of other goods and the war situation did not demand it. Organized by the Royal Hungarian Honvéd Institute of Military Technology, developments started in 1942, on the basis of broad cooperation. Within two years, a team of scientists organized by Professor Zoltán Bay, an industrial team by Edvin Istvánffy, and a military tasking and user team by Military Engineer Staff Corps Colonel Dr. József Jáky cooperatively built the prototypes of those radar variants that have been in use to the present day. Air surveillance radars already played a key role in the air defence of Budapest.

In the pre-war era, Hungarian and foreign physicists directed their interest toward the field of nuclear research and the study of microwaves. As there was neither industrial nor military need for nuclear research activities in Hungary, they remained in the realm of theory. This was not the case with microwaves, since there was an existing industrial background and civilian need for their use in the field of communications. The military need for the capability of determining the positions of aircraft in the dark, in fog, and through clouds prompted the start of research activities under the name of radiolocation in Europe, and radar (Radio Detection and Ranging) in the United States. Scientists in Hungary

[1] The Triple Helix model was introduced into the conceptual toolkit of innovation by Etzkowitz and Leydesdorff (1995).

stayed in the international “bloodstream” of scientific work right until the autumn of 1941, receiving American periodicals via the Netherlands (Philips) and Switzerland. However, all they were able to gather from them on the research conducted in this field was that in 1942, more than 50 percent of military electrotechnology development funds in the United States would be allocated to radars, while on-board aircraft radio systems would account for a mere 40 percent. Quite understandably, no more information was disclosed, being both military and industrial secrets, and thus, Hungary had to start the developments on its own, in complete isolation.

The process of basic research started with clarifying the principles of microwave communication technology and the workings of radars, then continued with building an experimental unit of a domestic radar. The initial engineering challenges were the excitation of microwaves on the shortest wavelength and with the highest power possible, as well as the reception and detection of microwaves with the lowest possible power, even in the presence of noise. The shortest possible wavelength was needed because whenever the wavelength gets reduced, microwaves increasingly take on the propagation characteristics of light. They propagate in a straight line, are not diffracted by the Earth, and are less reflected from the ionosphere or the clouds. Thus, they can be better directed and modulated as opposed to low-frequency radio waves, although they are less suitable for long-distance broadcasting.

Of the active elements used for generating forced oscillation, the only ones available on a domestic basis were electron tubes, although the operating principles of both magnetrons and klystrons were known to Hungarian developers. Given the short time frame and the limitations of available scientific engineering capacity, they did not even attempt to develop these devices. Instead, the members of Bay’s team of scientists – Ernő Winter, Zoltán Szepesi, and Andor Budincsevics – upgraded the new miniature tube type produced by the Egyesült Izzólámpa és Villamossági Rt. (United Incandescent Lamp and Electricity Ltd.), a company capable of developing and manufacturing already existing electron tubes. This was how the first microwave electron tube suitable for mass production in Hungary was created under the name EC 102. This electron tube’s output power was 2 W at wavelengths around half a metre (600 MHz), which already paved the way for experimentation with an experimental microwave transmitter and receiver and for the construction of a prototype, to be built by György Dallos.

The receiver unit needed for microwave communications also had a built-in EC 102 electron tube. The first experiments were carried out between the rooftop of the Tungsram building in Újpest and the Naszály Hill situated behind Vác, spanning a distance of around 100 km. As a result of the experiment, the scientists concluded that 50–100 mW transmitted power is enough for impeccable voice communication. The terrain features and buildings between the transmitter and the receiver obstructed the connection, while smaller trees and groves did not obstruct it, although they reduced the strength of the field. The scientists handed over their research results on microwave communications to Standard Electric Corp. for further use.

Telecommunications-related research results were also utilized during the development of radars. The experts not only proved that microwave propagation is not hindered by cloudy and foggy night-time weather conditions but also concluded that objects made of conductive materials – the physical dimensions of which are commensurable with the wavelength size – obstruct the propagation of microwaves. The discourse on theoretical issues of radiolocation measurement was based on the workings of a fire control radar. This is not by chance, since it was Colonel Jáky who already specified the military requirements.

Military Engineering Elements of the Ecosystem that Determine the Directions of Development

The basic air defence assets of the age were fighter planes and anti-aircraft guns. Setting requirements for the use of military radars was only necessitated by mass night bombing raids carried out during the Second World War, since the nighttime darkness not only hindered the interceptor aircraft from precise aiming but also complicated early warning and the location of attacking bomber formations.

The development of anti-aircraft artillery pieces has always kept pace with the evolution of aircraft. This "sword and shield" relationship determined the developments already during the First World War, when military aircraft with new capabilities and roles were appearing in theatres of war on almost a daily basis. To be able to detect and warn about them, the militaries established observation and listening posts and created a system by integrating these into a network adapted to the communication possibilities of the age. The technical means of air surveillance, however, were unable to keep pace with the emergence of ever-faster all-day aircraft with continuously increasing service ceilings. The development of anti-aircraft artillery assets started on the basis of the artillery pieces of the time. The configuration designed to ensure aiming and shooting at high angles of elevation – allowing 360-degree rotation of the gun fitted on a column mount – was invented relatively early on, but in that age, the barrel length of field guns and their low muzzle velocity were insufficient for hitting fast-moving aircraft flying at high altitudes. Therefore, the need arose for the development of gun barrels with longer calibres, projectiles with higher muzzle velocity, fragmentation count, and precision time fuses, as well as predictors, optical devices, and rangefinders.

After serious preliminary studies, the Hungarian Treasury purchased licences for the manufacture of 8cm L/50 calibre anti-aircraft guns (M 29) of the Swedish Bofors Works to destroy medium- and high-altitude air targets, and the Bofors licence for the manufacture of 40mm L/60 anti-aircraft autocannon (M 36) and its HE-FRAG shells against air targets attacking at medium and low altitudes with high angular velocity. These products met not only the then operational requirements but also the production technology capabilities of the domestic war industry.

Eliminating air targets over long distances requires very precise calculations. Complicating factors include, among others, not only the trajectory dispersion of active weapons but also the changes in target motion during the flight time of the projectile and the inaccuracies of their measurements, as well as the lengthiness of computing the set-forward point and transmitting the data. At first, the distances of air targets measured from the gun were determined with optical rangefinders, and these devices evolved significantly. However, the momentary slant range values did not and could not provide precise firing solutions. Thus, air defence artillerymen made estimates and used various command charts, which require the values of the elevation angle and the angular distance (azimuth). One can obtain a plot of the target by providing the slant range and the values of these two angles in a quick and precise way, periodically one after another; and the track of the target can be obtained by iterating this updating procedure. In the case of non-manoeuvring aircraft, one can calculate a speed and a bearing, and if the external ballistics of the gun is known, also a point of impact for the aircraft and the shell, so one can know the time of flight of the high-explosive shell, as well as the corresponding value to be set on its fuse. Insofar as one manages to successfully aim the gun at the target with the calculated lead distance, one must set this value on the fuse of the shell before loading it. The precise functioning of the fuse is key to achieving a high probability of hit. The bigger the speed difference between the target and the shell, the more precise ignition is needed. At first, this problem was solved with the use of small revolving-disc time fuses, but due to their poor reliability and low precision, they were considered only stopgap solutions. Under a German licence, the MOM[2] started to manufacture a small, wind-up delay-action fuse, which made it possible to achieve much higher precision. Hundreds of thousands of these fuses were produced before the war, with large quantities being exported to Great Britain.

Scoring a direct hit is not the most effective or economic method of destroying air targets, all the more so because it is much easier to bring the munition close to the target than to achieve a direct hit. Thus, besides accurate timing, it is also important that the fragment density created by the detonation in the vicinity of the target ensures a target kill.

HUMAN ASPECTS OF DEFENCE INNOVATION

Prominent Figures in Science and Industry

In Germany, intensive research to develop military radars started in 1939–40. Hungarian military leaders were well aware of two facts: Hungary would not receive any help from its ally, and modern air defence without radars is unthinkable. The very realization of these facts already presupposed the involvement of military engineers of the first pillar and the expert staff of the Institute of Military Technology (IMT), as it was laid down in its founding charter.[3] In 1941, the Institute of Military Technology was already working out the Common Military and Technical Requirements (HMK) of radars. They gathered information about the results of engineering sciences, the lessons learned abroad, and the capabilities of domestic universities and industry. On 25 January 1942, they submitted a report to the minister of defence, in which they already considered it a fact that the Bay team was to be formed, and specified its initial composition in the annex, together with its mission and remuneration.

Altogether 150,000 pengős were earmarked for financing the Bay team, whereas 400,000 pengős for the production of the four Sas (Eagle) radars. Thus, the Bay team was still being formed when the IMT had already worked out the costs of the basic experiments. The industrial team (led by Edvin Istvánffy) did not even get a mention, but based on the HMK, the IMT had already calculated the costs of the four Sas radars in cooperation with the industrial team. Although Jáky's appointment as ministerial commissioner took place no sooner than in March 1943, this authorization made him the commander of both the Bay team and the industrial participants. Besides enabling him to assign tasks to all players in the defence innovation ecosystem, the authorization also gave him the opportunity to save people and war industry equipment during the German occupation and the rule of the Arrow Cross Party.

[2] This factory was renamed Hungarian Optical Works (MOM) in 1939. Its founder, the Germany-born Ferdinand Süss managed the MOM until the end of the Second World War.

[3] "The Institute of Military Technology has been established as an organ of the Royal Hungarian Ministry of Defence with the mission of representing, in an economical way, the advancement of technology in the supply of the army with weapons, armaments and other equipment."

It was György Papp, Károly Simonyi, and Antal Sólyi who started the work of the Bay team, the second pillar. Instead of a request, the Bay team was formed on the basis of an order provided by the laws in force. Nobody was asked whether they wanted to join or not. They had to give answers to some fundamental questions. How much transmitted energy is needed to make sure that a sufficient amount of energy returns? What should the bandwidth be, and what is the optimal pulse length for the signal?

According to the worked-out theory, a microwave, a short and high-power pulse packet emitted by a transmitter, is sent towards an aircraft with the help of a directional antenna. Then, the low-power echo signals reflected from the aircraft surface in the direction of the antenna are fed into a sensitive receiver unit. The slant range between the place of transmission and the aircraft can be calculated from the time delay from transmission to reception, by taking into consideration the propagation velocity of electromagnetic waves. The antenna's axis points to the aircraft, so its deviation from the northern and horizontal directions provides two angular values. Knowing the place of transmission, one can determine the spatial coordinates of the aircraft using these two angular values and the slant range.

By the spring of 1943, the team had built an experimental radar and used it to detect barges on River Danube and aircraft from atop the Egyesült Izzólámpa és Villamossági Rt's building. The microwave transmitter needed for this purpose was constructed by Ernő Winter and Andor Budincsevics. The third pillar already contributed to the creation of this experimental device. The scientists set up another experimental unit on the top of the Standard building to experiment with microwave signal transmission, which was more convenient than relocating to Naszály Hill in Vác on each occasion and making contact with Újpest from there.

Although Standard and Edvin Istvánffy formed the centre of the third pillar, several other companies were also involved in the manufacturing of radars, such as the Egyesült Izzólámpa és Villamossági Rt., MOM, Gamma, the Hungarian Wagon and Machine Works, Telefunken, Philips, BAMERT, and a number of small enterprises. All players were expected to maintain complete secrecy and loyalty, so it is no wonder that the work almost stopped after 19 March 1944, the day of the German occupation. The IMT radar team was relocated to Nógrádverőce, which was a safer place, but its members could not do any work there due to the unsuitable electrical grid.

Military Engineer Officers

As the contemporary saying goes, military engineers do not grow on trees. This was the case after Trianon, too. Neither military engineer training, nor military technology research and development did the Austro-Hungarian Monarchy let slip out of its reach. As both were important parts of the independent Hungarian statehood, the Institute of Military Technology was established in 1920, and young officers were enrolled in various engineering programs of study, characteristically at the Royal Hungarian "Palatine Joseph" University of Technology. After graduation from the basic training, they were supposed to take military engineering and then Military Engineer Staff Corps courses. Students with worse than excellent exam results were rarely admitted among the engineers of the Institute of Military Technology. Teachers realized the officers' triadic training goal by mentoring talents in the fields of engineering science and complementing their studies with military knowledge so that they can be integrated into all three pillars. Officially, we are told that the Győr Program of Hungary's rearmament was launched in 1938. In my opinion, that year saw only the financial resources being allocated to it. The (innovation) process necessary for the Program started as early as the first young and talented soldiers were schooled to make sure that in 10–20 years, a sufficient number of military engineers would be available for the developments.

Unfolding Talent

József Janicsek was born in Eperjes (today Prešov, Slovakia) on 26 March 1897. He magyarized his name to Jáky in 1934. On 13 November 1915, he volunteered to enlist in the Imperial and Royal 34th Infantry Regiment, with which he deployed to serve on the Russian front for six months. He was ordered to attend the second year of the mechanical engineer specialization at the University of Technology in 1921, and in addition, he had to fill a teaching position at the Ludovika Academy as well.

When the Royal Hungarian Institute of Military Technology was officially established in 1930, he was appointed head of the IMT electronics laboratory. He built and headed this laboratory for eight years, where the core components of innumerable IMT-developed, wired and wireless devices were made. As of 1 October 1938, he was appointed head of the IMT Special Department No. 4. In 1941, he doctorated in engineering sciences after submitting his thesis on “the electronic methods of measuring projectile velocity”.

Thanks to his scientific work and radio developments, he personally knew the members of the Hungarian engineering elite of the time, as he was collaborating and researching with them or learning from them. The theoretical foundations of radiolocation were already known at that time, and researchers had access to foreign special literature until the end of the 1930s. The construction of the first operable radars, however, was shrouded in complete secrecy. Although Jáky participated in study tours to Germany on two occasions, the German side did not share any technical information, and the issue of radars was shrouded in such secrecy even in Hungary that Jáky’s immediate colleagues only knew that he was researching this issue, but were not let into the details.

SCIENTIFIC AND INDUSTRIAL ACHIEVEMENTS AT THE IMT

The Council of Scientific Engineering at the IMT was already functioning in 1938–39, with Dr. Zoltán Bay among its members. Back then, scientists were investigating the effect of the ionosphere on the propagation of radio waves, and they also came up with the idea of radar already at that time. Jáky applied for the newly organized Communications Technology Department of the University of Technology in 1944. Dr. Zoltán Bay was a member of the nomination committee. Of several applicants, the committee nominated Dr. József Jáky as the Teacher of Communications Technology at the University of Technology.

Sas (Eagle) Air Surveillance Radar

In January 1943, acting on the IMT’s proposal, the Ministry of Defence placed an order with Standard for four Sas (Eagle) radars. In those times, Hungary had already been producing and delivering electronic components, for German radars among others, and received promises of German radars to be delivered in exchange, but the German side refused to hand over the manufacturing documentation belonging to them. They had good reason to do so since they knew that we could have used the information contained in those documents for our own developments. Nevertheless, the construction of Sas radars was proceeding at a great pace, and the first installations started already in November 1943.

The first Sas was set up next to the lookout tower on János Hill. The detection range of meter-wave radars is, to a large extent, affected by the reflection of the surrounding, preferably flat area of land. As this was not given at the hilltop, the experts soon rejected this installation site and, acting on Jáky's proposal, relocated the radar unit to the experimental premises of the IMT in Sári, so that they could take part in the control of three Würzburg D radars already operating in the fire system of Budapest. The next two Sas radars were scheduled to achieve operational readiness by the spring of 1944, and the MoD planned to install them at a site in Jászkisér. For defence against the attacking Anglo-American formations, this did not seem a good choice from an operational point of view. It is no accident that subsequently, Lovasberény also emerged as another installation site, and the radar sets were relocated there on an unknown date. The Sas radars were set up in pairs. While one of them performed omnidirectional surveillance, rotating at three revolutions per minute, the other performed a sector scan in the main direction. According to oral recollections, the Sas radars were able to detect air targets already above the Adriatic Sea (400–500 km). Knowing the transmitted power of the instrument, this seemed no more than a legend until the appearance of István Balajti's article in the periodical Haditechnika,[4] in which he called attention to the fact that the Sas radars were installed in a so-called quasi-monostatic configuration. Set up in pairs, the transmitted power of the two Sas radars, the gains of their transmitter and receiver antennas, as well as the echo signals reflected from the target surface, were integrated, which doubled the detection range of the radars.

Thanks to the fulfilment of operational conditions, the three pairs of Sas air surveillance radars – set up respectively on the premises of the IMT in Sári village, in Jászkisér, and then in Lovasberény – significantly contributed to the early warning of the population of Budapest on the occasion of air raids, and thereby saved many lives.

Installation Sites of the Sas Radars

After the experiment on János Hill, the first two Sas radars were set up on the premises in Sári village and started operating in November, controlling the three Würzburg D radars integrated into the Budapest fire system. In his book, based on the residents' recollections, Pál Szabó estimated that the installation site was approximately 8 kilometres from Sári in the direction of Mántelek.[5] This contradicts the drawings of the installation sites, Captain László Sifter's recollections, and the photo published by him, but first and foremost, it contradicts the fact that there was no suitable electrical grid available on the location referred to in Szabó's book and its establishment incurred substantial costs and required planning and implementation work on every other installation site. Without disputing the reminiscences of local residents, the site and the circumstances of the construction they described did not meet the requirements for setting up an air defence radiolocation battery. There must have been something there indeed, but it certainly was not the installation site of Sas radars. The facility on Sári premises was camouflaged as a small garden at the end of the village. Jászkisér is referred to as an installation site in several documents, and the construction of

[4] Balajti 2021, 8–15.

[5] Szabó 2014.

the site and the installations were in progress indeed, so much so that even a trial run took place there, but so far, we have not found any drawings or photos. Considering the directions of attacks by Anglo-American bomber formations, this installation site seems to be a bad choice from an operational point of view, as it could not provide information about these formations to the Budapest fire system. In his article, Captain László Sifter makes specific mention of the operation of repaired Sas radars on the Lovasberény installation site in the interest of the air defence of Budapest.[6]

Borbála Fire Guidance/Control Radar

The Borbála and the Bagoly radars were almost completely identical in terms of their technical content, but their radar antennas were totally different due to the diverse requirements. The parabolic reflector of the Borbála radar was a concave copper plate dish measuring 3 metres in diameter, whereas the antenna of the Bagoly was an array with a diameter of 7.5 metres. The Borbála was manufactured at Standard Corp. under Edvin Istvánffy's supervision. Because the instrument package of the Bagoly was identical with that of the Borbála, the construction of Bagoly radars also required successful work on the part of Standard. While Jáky commissioned the Gamma and Ganz companies to develop the actuator of the Borbála radar, he assigned the task of building a prototype of the reflector to a craftsman. On 23 April 1943, the experts installed the first unit of the Borbála radar on the rooftop of an Egyesült Izzólámpa és Villamossági Rt. building, and started measurements with an air target flying to and fro over River Danube on the route Budapest–Vác. In July 1943, already three Borbála radar devices were being manufactured by Standard, and the Ministry of Defence allocated to the factory three autocannon carriages with reinforced wheel structures for the radars.

Bagoly (Owl) Fighter Control Radar

As ministerial commissioner, Jáky commissioned the Győr Wagon and Machine Factory to manufacture the structure of the Hungarian fighter control radar. At a meeting held on 14 May 1943, the factory was represented by CEO Imre Pattantyús-Ábrahám. Captain Dezső Ritter, a member of the military engineering development team, was present on behalf of the IMT. The participants divided the work process into three main phases: the supervision and drawing of the radar design, the production of components, and the assembly of component parts. As the radar was a bulky device with instrument-level precision, the factory could not undertake this work, which required a company or person specialized in instrument design and manufacturing. The factory undertook to manufacture some, mostly major, parts and to provide the assembly site. Jáky understood and accepted the reasons, so he made arrangements to expand the negotiations by involving experts from Standard and Gamma. Thus, Standard now had a stake in designing/manufacturing the complete electronics of the radar, whereas Gamma in that of the precision mechanical components. At that point, it was already clear that the domestic fighter-control radar would certainly not be completed in 1943, and as a matter of fact, two Bagoly radars outlived the end of the war in an assembled but uninstalled condition.

[6] Sifter 1948, 48–49.

Turul Airborne Radar

The British night bombing raids against Germany prompted Hungarian military leaders, too, to find a solution to countering them. Introducing measures for complete night blackout seemed an evident solution, yet it proved to be insufficient due to the increasingly precise navigation and the dropping of illumination bombs slowly descending with parachutes. Neither did the illumination of the night sky with searchlights for the anti-aircraft artillery lead to the desired efficiency. After the Bay team worked out the theoretical foundations, in view of the foreseeable military requirements, the Institute of Military Technology and the Institute for Aviation Experimentation launched a joint development project to construct a radar-equipped night fighter plane on the basis of a domestically manufactured Me 210, since there was no chance of any German delivery, like in the case of fire control and air surveillance radars. The experimental radar prototype was completed at the Hungarian Philips Works by 19 March 1944 and was built into a Me 210D destroyer with side number ZO+03 in the place of the bomb bay. There are no extant data about the experimental flight of the onboard aircraft radar codenamed Turul and its result.

Würzburg D (Dora) Tracking Radar

Although the Borbála radars were completed, their constructors with anti-fascist sentiments certainly did not hand over or develop anything during the German occupation. The Germans were definitely not interested in the successful completion of Hungarian developments. Under the earlier contract, 3+1 German Würzburg D radars were delivered. According to the plans, when installed on location in the corner of Megyeri cemetery, on Kis-Sváb Hill, and in the northern part of Csepel, they constituted a part of Budapest's fire system. As the Dora radars were mobile and it was necessary to train the Hungarian crew as well, they turned up in several places. Some remember the Megyeri installation site, which Professor Bay also attempted to visit. There are some built remains of the Kis-Sváb Hill installation site, which was integrated into a nature conservation area, and there is an extant photo of a radar installed at the junction of Mexikói Road and Szőnyi Road, where the site was used for training purposes, but their further fate remains unknown.

The 272nd Air Defence Radiolocation Battery in Dunapentele

On 18 May 1943, a meeting was held to organize the construction of a fighter control post. Large-scale night air raids against Germany were already going on, and the Hungarian military leaders were attentively monitoring them. Considering that this already touched a nerve among German interests, and given that the production of Hungarian Bagoly radars was not yet finished, we were promised to have one Freya early warning and two Würzburg-Riese fighter control radars delivered to us. Although the delivery was scheduled to take place in early April, the radars did not arrive before late May or early June. One suspected direction of the attack was in the Danube Valley from the south, and that is why Dunapentele was chosen as an installation site. The meeting was summoned by Jáky with the purpose of discussing the selection of participants, the budget, the appropriation of the area, and the contract of the constructor of the post. The chosen area was the first element in a countrywide network, but no data have been found on the construction of other elements. The installation site was located southeast of Dunapentele, at spot elevation 153, and Telefunken Corp. was commissioned with the construction.

During the construction of Dunaújváros, the area in question was completely transformed, but the Trinity Church of Dunaújváros can still be seen on period draft maps, so one can find its location. This area corresponds to the site of today's Theme Park. The three radars were needed because target aircraft were identified based on data from the air surveillance radar, and then one of the fighter-control radars took over the tracking of the aircraft, while the other was tracking its own night fighter plane. The data were presented on a Seeburg Tisch (plotting board). The radio communications of the post were planned with German FuG16 and Hungarian R7/a and R/14 radio sets, and Jáky also had a crucial role in their development.

The two Würzburg-Riese radars were delivered in June, to be followed in September by the Freya early warning radar for their control, but these radars came with some of their parts missing, and the construction of the post was not completed by the deadline. On 20 December 1943, Jáky reported that the 272nd Air Defence Radiolocation Battery in Dunapentele was ready for operation.

The Development of Surface-to-Air Missiles in 1944

Acting on the order of Major General Zoltán Hihalmi Harmos, Colonel Jáky held a discussion in his office on 12 August 1944 with the participation of experts from the Institute of Military Technology, Standard, and the MOM. The topic of the meeting was "remote control of glide bombs". Jáky revealed that the efficiency of conventional tube anti-aircraft artillery was no longer satisfactory and that there was an opportunity to find a revolutionary new solution based on a MOM patent. Deputy CEO of MOM, Mr. Grosh, noted that the mechanical components of the steering system had already been designed, the servomotor was ready, and could be tested in the wind tunnel of the University of Technology in three months. Speaking on behalf of Standard, Edvin Istvánffy asked for a moratorium due to the radar program, which he did not consider a hindrance, as both the radar and the range finding were solved issues. IMT expert First Lieutenant Takács told the participants that the authorized divisions of the IMT would start experiments for the construction of solid-fuel and bipropellant liquid (hydrogen/oxygen) variants of a missile with an effective range of 10–20 km.

Jáky convened another technical advisory meeting on 17 August, inviting Károly Bors, who was to be tasked with the design of the control unit of the observation station. It was recorded in the minutes that the participants did not wish to share the current state of the development with their allies – less than five months after the first day of the German occupation. This development topic is of present interest also because it shows that – provided they exist and are interconnected – the elements of the defence innovation ecosystem may bring about revolutionary achievements.

MILITARY ENGINEERS AND ANTI-FASCIST RESISTANCE

Jáky's task in the group led by Endre Bajcsy-Zsilinszky would have been to construct a high-performance radio set that would have enabled the members of the group to get in touch with the Soviet Army Headquarters to avoid the siege of Budapest. Captain Andor Lányi also came to his assistance in building the 5-kW transceiver. Pál Almásy – who had first met Jáky on the Hajmáskér shooting range – was tasked with recruiting anti-German officers into the resistance group led by János Kis. The tasks were assigned to them by the later mayor of Budapest, József Kővágó.

Altogether, two devices were built in the IMT, and the components of the second were accounted for as spare parts. The radios had been completed by early December 1944. Although the resisters tried to transport a radio to the planned site, the truck driver drove on when he spotted some Germans, who had already uncovered the planned installation site of the transceiver. There is no extant data on the further fate of the radio station. Following the relocation of the IMT from Budapest, Jáky, together with several other resisters, stayed in the Hadik barracks. The IMT was ordered to relocate to Rábafüzes, and then to Szombathely. Jáky was supposed to go to Dresden, but he and the others stayed home, keeping up the semblance of an official unit using documents and stamps stolen by Engineer Staff Corps Colonel Béla Cserneczky. Colonel Cserneczky undertook to take command of the remaining cell. His task in Endre Bajcsy-Zsilinszky's group would have been to prevent the demolition of bridges over River Danube. To this end, he gave 100 kg of explosives to the resistance movement and manufactured 1000 detonators without charges to replace the ones the Germans had planted on the bridges. In late November, the resistance movement was discovered, and he was unable to conduct any activities anymore. Several military engineers, scientists, and soldiers specialized in development and production wrote in their memoirs that everything changed after 19 March 1944, the day of the German occupation. Developments were halted, not only because their management and financing were stopped but also because the moral ground of further works was called into question. From that point on, these works served the interests of a foreign power rather than homeland defence.

CONCLUSION

By the spring of 1944, thanks to the availability of all necessary elements of the defence innovation ecosystem and their planned management, Hungary was capable of producing radar prototypes belonging to cutting-edge science and technology in the world, and commissioning and operating four Sas air surveillance radars.

The existence, workings, and management of the elements of the defence innovation ecosystem are not self-evident. The development of the military industry did not start with the Győr program, it rather started with the training and organization of military engineers as a key component. During the German occupation, everything changed in Hungary. Among the things that ceased to exist were the moral ground, the governmental intention, and with it, the will operating the pillars of defence innovation, and then the cooperation among its three crucial pillars.

Military engineering knowledge forms the basis of successful research and development in military technology. Jáky's knowledge of military technology set requirements for Professor Zoltán Bay's team of scientists and Edvin Istvánffy's industrial engineers during the process of creating the Sas radar. Professor Tódor Kármán, the founder of the Advisory Group for Aerospace Research and Development (AGARD) – who earlier worked on the development of PKZ helicopters at the research institute of the Austro-Hungarian Monarchy – recognized this law and formulated it in the Scientific Advisory Board of the USAF: "scientific results cannot be used efficiently by soldiers who have no understanding of them, and scientists cannot produce results without an understanding of the operations".[7]

[7] Van der Bliek 1999, 1.

The results of defence innovation and their utilization involve many industrial and military secrets, and therefore, the key issue is that they should offer advantages on the battlefield and market. This goal can be achieved only through cooperation. The goal of making good use of the "secret" wherever it is needed requires joint research teams, laboratories, and testing grounds of science, industry, and national defence. Loyalty – to the state, to the alliance – is the cohesive force holding them together, being the moral ground of defence innovation. If this cohesive force ceases to exist or changes, defence innovations will not be utilized at all, or not in the place intended by the original will.

The most significant defence developments are always connected with some outstanding talent. On examining the talents' career paths, we always find that the process of planned talent mentoring built on a central will is present. It is especially true of the education of military engineers, where the needed outstanding talents not only know the state of the art in science and industry but are also able to creatively use their knowledge in a rapidly changing security environment. Industry 3.0–5.0 and Education 4.0 programs might be related to but are too broad to fit into the scope of the current study, therefore, I suggest this topic as a basis for another paper.

BIBLIOGRAPHY

- Balajti, István: A rádiófrekvenciás radarhálózatok előnyei és megvalósításuk kihívásai [Advantages of Radio Frequency Radar Networks and the Challenges of Their Implementation]. Haditechnika, Vol. 55, No. 5 (2021), pp. 8–15. http://real.mtak.hu/132360/1/HT_2021-5_cikk_02.pdf (Downloaded: 28/10/2023).
- Balajti, István – Hajdú, Ferenc: Surprising Findings from the Hungarian Radar Developments in the Era of the Second World War. URSI Radio Science Bulletin, No. 358 (2016), pp. 82–108.
- Dr. Barczy, Zoltán – Sárhidai, Gyula: A Magyar Királyi Honvédség légvédelme, 1920–1945 [The Air Defence of the Royal Hungarian Defence Forces]. Zrínyi Publishing House, Budapest, 2010, ISBN 978 963 327 498 9, pp. 498–499.
- Bay, Zoltán: Az élet erősebb [Life is Stronger]. Csokonai–Püski, Debrecen–Budapest, 1990. https://mek.oszk.hu/15800/15845/15845.pdf (Downloaded: 29/05/2023).
- Bay, Zoltán: Hazai mikrohullámú kísérletek [Microwave Investigations in Hungary during the Second World War]. Elektrotechnika, Vol. 38, No. 6–8 (1946), pp. 29–40. https://www.mee.hu/files/files/ssd2/ET/1946/ET_1946_06-08t_hp.pdf (Downloaded: 29/05/2023).
- Etzkowitz, Henry – Leydesdorff, Loet: The Triple Helix – University-Industry-Government Relations: A Laboratory for Knowledge Based Economic Development. EASST Review, Vol. 14, No. 1 (1995), pp. 14–19.
- Dr. Hajdú, Ferenc, PhD: Triális képzés a had és hadiipari mérnökök új generációi számára – A védelmi innováció újraindítása [Triadic Training for New Generations of Military and Defence Industrial Engineers – The Restart of Defence Innovation]. Haditechnika, Vol. 56, No. 6 (2022), pp. 61–63. https://kiadvany.magyarhonvedseg.hu/index.php/HT/article/view/1029/961
- Istvánffy, Edvin: Hazai és külföldi radarkészülékek [Home and Foreign Made Radars]. Elektrotechnika, Vol. 40, No. 1 (1948), pp. 1–12. https://www.mee.hu/files/files/ssd2/ET/1948/ET_1948_01t.pdf (Downloaded: 26/10/2023).
- Sifter, László: Magyar radarkészülékek [Hungarian Radar Devices]. Honvéd, No. 1 (1948), pp. 48–49.

- Szabó, Pál József: Radarokkal a lopakodók ellen [With Radars Against Stealth Aircraft]. Zrínyi Publishing House, Budapest, 2014. ISBN 978 963 327 621 1.
- Van der Bliek, Jan (ed.): AGARD – The History 1952–1997. The NATO Research and Technology Organization, 1999. https://apps.dtic.mil/sti/tr/pdf/ADA396959.pdf

Szabolcs Lóránt

STRENGTHENING EUROPE'S DEFENCE INDUSTRIAL BASE: ANALYSIS OF THE EDIP FRAMEWORK

DOI: 10.35926/HDR.2025.1.3

ABSTRACT: *This article analyses the European Defence Industry Programme (EDIP), a landmark EU regulation proposed in early 2024 and currently under discussion by the European Parliament and Council, that marks a fundamental shift in European defence industrial policy. Moving beyond emergency responses to Russia's invasion of Ukraine, EDIP introduces comprehensive mechanisms for strengthening the European Defence Technological and Industrial Base. Through analysis of the draft Regulation's primary sources, the study examines how EDIP establishes permanent structures for defence industrial cooperation, including the innovative Structure for the European Armament Programme framework, sophisticated supply chain security measures, and mechanisms for Ukrainian defence industrial integration. The article argues that EDIP represents a strategic transformation from voluntary coordination to the active management of defence industrial capabilities, creating flexible yet robust frameworks for long-term European defence industrial development. While implementation challenges remain, particularly regarding security requirements and institutional coordination, EDIP establishes foundations for a more integrated European defence industrial base that will likely shape policy evolution beyond its initial 2025–2027 timeframe.*

KEYWORDS: *European Defence Industry Programme (EDIP), defence industrial policy, Ukraine's integration, industrial cooperation, European Defence Technological and Industrial Base*

ABOUT THE AUTHOR:

Szabolcs Lóránt is a reserve military officer (lieutenant) at the Hungarian Defence Forces, a PhD candidate at Ludovika University of Public Service, and a former EU attaché (ORCID: 0009-0005-1707-0544, MTMT: 10095006).

INTRODUCTION

The renewed debate about NATO defence spending targets intensified in early 2025. During his first week back in office, U.S. President Trump called for allies to spend 5% of their GDP on defence,[1] while newly appointed NATO Secretary General Mark Rutte suggested moving "north of 3 percent". French President Emmanuel Macron, while acknowledging that France's current 2.06% might be insufficient for a "major confrontation", insisted that

[1] Hunnicutt 2025.

the increased European defence spending must primarily benefit the continent's industrial base rather than American companies.[2]

These discussions, however, often oversimplify Europe's defence industrial challenges. When Rutte declares that "the problem is not Trump or the US, the problem is Europe",[3] arguing for a "war mindset" in military spending, he seems to overlook how Europe's security dependency stems from complex industrial, technological factors and the transatlantic relations developed over decades. The fragmentation of European defence production – with 62 different land warfare platforms compared to America's eight, and 47 naval warfare platforms versus six in the U.S., as Macron recently highlighted – illustrates the scale of industrial inefficiency.

The European Defence Industry Programme (EDIP) addresses these fundamental challenges by introducing comprehensive measures for industrial integration, supply chain resilience, and production capacity enhancement. Rather than merely increasing spending, EDIP aims to transform how Europe develops, produces, and maintains its defence capabilities through innovative institutional and regulatory mechanisms.

STRATEGIC CONTEXT

EDIP represents a landmark shift in EU defence industrial policy, marking the transition from emergency responses to a comprehensive approach for long-term industrial readiness.

EDIP, which is currently a proposal tabled by the European Commission as a Regulation and under discussion by the European Parliament and Council, aims, as its name suggests, to strengthen the European Defence Technological and Industrial Base (EDTIB),[4] ensuring the timely availability of defence products and supporting Ukraine's defence industry integration.

The introduction of EDIP responds directly to the transformed security environment following Russia's invasion of Ukraine, which has exposed critical vulnerabilities in Europe's defence production capabilities.[5] As outlined in Article 1 of the proposed Regulation, EDIP establishes both a budgetary framework and a comprehensive set of measures addressing five key areas:

- The core Programme supporting EDTIB competitiveness and ensuring that European defence companies produce and deliver military equipment when needed,
- Ukraine Support Instrument for defence industrial integration,
- Structure for European Armament Programme (SEAP) for joint procurement,
- Security of Supply regime with crisis response mechanisms,
- Defence Industrial Readiness Board for coordination.[6]

[2] Kayali 2025.

[3] Bloomberg [@business] 2025.

[4] Note: the European Defence Technological and Industrial Base represents the collective defence industry capabilities and technological know-how within the European Union.

[5] European Commission: Staff Working Document 2024, Section 1.

[6] European Commission 2024a (EDIP Regulation), Article 1.

FINANCIAL FRAMEWORK AND TIMELINE

With a dedicated financial envelope of €1.5 billion for 2025–2027 (Article 5), EDIP bridges a critical gap between current emergency measures – Act in Support of Ammunition Production (ASAP) and European Defence Industry Reinforcement through common Procurement Act (EDIRPA), which expire in 2025 – and future long-term initiatives under the next Multiannual Financial Framework (2028–2034). As detailed in the Staff Working Document (Section 7.8), while this amount remains modest given the challenges faced, it ensures continuity in EU support for defence industrial adaptation. In addition, the EDIP Regulation allows flexible budget distribution across measures, enabling quick responses to geopolitical changes and Member State needs, with the Commission setting priorities through work programmes in coordination with Member States (in the EDIP Programme Committee) and the Defence Industrial Readiness Board.[7]

EDIS–EDIP RELATIONSHIP

The European Defence Industrial Strategy (EDIS)[8] and the European Defence Industry Programme (EDIP) represent complementary elements of the EU's renewed approach to defence industrial policy. EDIS serves as the overarching strategic framework, providing a comprehensive vision for strengthening Europe's defence industrial capabilities. Meanwhile, EDIP functions as the primary implementation mechanism, equipped with concrete funding, although only a modest amount for the time being, and tools to realize these strategic objectives.

EDIP comes with a dedicated budget of €1.5 billion for investing in the defence industrial readiness and competitiveness of the EDTIB. This funding serves as a bridge towards more ambitious financial commitments anticipated in the next EU budgetary cycle starting in 2028. The program builds significantly on previous EU defence initiatives, particularly EDIRPA[9] and ASAP.[10]

In brief, the EDIS sets the overarching vision for achieving EU defence readiness through a responsive and resilient defence industry, while EDIP provides the concrete mechanisms and €1.5 billion funding to begin implementing this vision during the current Multiannual Financial Framework. Through its support for industrial ramp-up, joint procurement, and defence cooperation, EDIP serves as the immediate operational instrument for realizing EDIS's broader objectives of increasing defence readiness, ensuring security of supply, and strengthening the EDTIB.

[7] European Commission: Staff Working Document 2024, Section 7.8.

[8] European Commission 2024b (EDIS).

[9] Note: EDIRPA supports joint EU/Norway defence procurement (€310M total) through funding streams for Ammunition, Air/Missile Defence, and Legacy Systems (€103.2M each). EU funds cover cooperation costs, not procurement.

[10] Note: ASAP aims to boost the EU defence industry manufacturing capacity for ammunition and missiles through 5 funding calls (explosives, powder, shells, missiles, and testing/certification), with €500M EU funding leveraging industry co-financing to €1.4B total. It operates as Track 3 of the EU's ammunition plan, complementing Track 1 (immediate ammunition transfer from existing stocks to Ukraine) and Track 2 (joint procurement to replenish stocks).

CURRENT DEFENCE INDUSTRIAL MEASURES

This overview of the current EU defence industrial measures that form the baseline scenario before EDIP can help us understand the context and evolution of the EU defence industrial policy. Currently, there are four main instruments in place, each serving different but complementary purposes.

EUROPEAN DEFENCE FUND

The European Defence Fund (EDF), established in 2021, represents a mature evolution of the EU's defence research and development initiatives, building on earlier pilot programs like the Preparatory Action on Defence Research (PADR) and the European Defence Industrial Development Programme (EDIDP). With a precisely allocated budget of €7.953 billion for 2021–2027, the EDF operates through a dual-dimension approach: funding collaborative defence research through grants (roughly one-third of the budget) and co-financing capability development projects (approximately two-thirds) that complement Member States' investments.[11]

Established by Regulation (EU) 2021/697, EDF's governance structure reflects its strategic importance. While the European Commission maintains direct management authority, the Program Committee, comprising the Member States as voting members, plays a crucial role in establishing work programs and setting multi-annual perspectives. The European Defence Agency (EDA) and the European External Action Service (EEAS) contribute their expertise as observers, with EDA taking on additional responsibilities since 2022 as an implementing partner for the indirect management of certain actions. This includes grant management, implementation monitoring, and financial oversight of specific projects.[12]

The EDF 2024 work program[13] exemplifies the Fund's comprehensive approach, addressing 32 call topics across critical defence domains while allocating €225 million to the EU Defence Innovation Scheme (EUDIS). This systematic investment in collaborative defence R&D, complemented by specific support measures for small and medium-sized enterprises (SMEs) and startups, demonstrates how the EDF has evolved from its experimental predecessors into a cornerstone instrument for fostering European defence technological and industrial cooperation.

JOINT PROCUREMENT TASK FORCE AND EDIRPA

The EU developed two complementary instruments to bridge immediate defence procurement needs with longer-term strategic objectives. The Defence Joint Procurement Task Force (DJPTF), established in response to the May 2022 Joint Communication on Defence Investment Gaps, represents the first step in this approach. The Task Force brings together expertise from across EU institutions – including the EEAS, EDA, and the European Commission – to create an agile coordination mechanism. It systematically maps and harmonises Member States' short-term procurement needs across seven critical equipment

[11] EDF Webpage 2025.

[12] EDA Webpage 2025.

[13] EDF Webpage 2025.

categories, ranging from medical supplies to air defence systems, while assessing the European defence industry's capacity to meet these requirements.[14]

Building on the Task Force's analytical groundwork, EDIRPA was adopted in October 2023 as a more structured intervention mechanism. With a dedicated budget of €310 million, aimed at covering the cooperation costs related to common procurements, EDIRPA transforms the Task Force's coordination efforts into concrete financial incentives for joint procurement in three priority areas: ammunition, air and missile defence, and platforms/legacy system replacement.[15] While EDIRPA operates under a defined timeline through 2025, this temporary nature serves a strategic purpose: it allows the EU to test and refine cooperative procurement approaches that can later be incorporated into more permanent structures under EDIP.

Together, these instruments demonstrate the EU's multi-layered response to defence industrial challenges: the Task Force provides immediate coordination and market intelligence, while EDIRPA offers financial tools to stimulate joint procurement. This combination helps prevent procurement conflicts among Member States while simultaneously building patterns of cooperation that can be institutionalized in more permanent frameworks. Their sequential development also reflects a learning approach, where lessons from informal coordination through the Task Force inform the design of more structured mechanisms in EDIRPA, which in turn shapes the development of long-term instruments.

ASAP

A critical component of the EU's defence industrial response has been the Act in Support of Ammunition Production,[16] adopted in July 2023. This instrument emerged directly from the lessons learned during Russia's war on Ukraine, which highlighted critical vulnerabilities in European ammunition production capacity. ASAP represents the EU's targeted response to this challenge, allocating €513 million (leveraging to €1.4 billion total investment) specifically to increase ammunition and missile production capacities. The program has already demonstrated concrete results: the EU artillery ammunition production capacity has increased from the pre-war baseline to reach 1 million rounds annually by January 2024, with a target of 2 million by the end of 2025.[17]

However, ASAP's scheduled expiration in June 2025, coinciding with EDIRPA's end date, creates a critical temporal challenge. This impending "support gap", identified in Section 5.1 of the Commission's Staff Working Document, becomes particularly problematic given the ongoing nature of the conflict in Ukraine and the continuing need to both support Ukraine and replenish European stockpiles. This temporal discontinuity helps explain both the urgency and the comprehensive scope of the proposed EDIP, which aims to ensure sustained support for European defence industrial capacity building beyond these temporary measures.

[14] European Commission: Staff Working Document 2024, 36–37.

[15] European Commission 2023.

[16] EU 2023.

[17] European Commission 2024c.

FROM EMERGENCY RESPONSE TO SUSTAINABLE FRAMEWORK: EDIP'S ROLE

To sum up, EDIP builds on existing initiatives by extending EDIRPA's joint procurement approach beyond 2025 and replicating ASAP's production support model. It introduces SEAP (analysed in detail in the section "Structure for European Armament Programme" below) as a flexible cooperation framework enabling collaborative procurement, full lifecycle management (from initial acquisition to decommissioning), and dynamic availability management through readiness pools. The program ensures EDF-developed technologies move from research to actual production and market deployment through repayable grants while introducing new financial mechanisms like FAST to support SMEs and small midcaps in industrial capacity expansion.

EDIP represents an evolution from ASAP and EDIRPA's emergency-focused interventions to a more systematic approach to EU defence industrial preparedness. While ASAP addressed urgent ammunition production needs and EDIRPA incentivized joint procurement of critical defence products, EDIP establishes a comprehensive framework that extends these successful mechanisms while introducing new elements. These include the security of the supply regime for crisis response, the SEAP framework enabling Member States, associated countries, and Ukraine to form flexible configurations for specific defence programs, and support for EDF project commercialization. By institutionalizing and expanding these tools, EDIP creates a more sustainable approach to strengthening the EDTIB.

EDIP CORE ELEMENTS

Institutional Innovations

Defence Industrial Readiness Board

The Regulation creates a new institutional architecture for European defence industry coordination through the Defence Industrial Readiness Board (Article 57). The Board operates with two distinct but complementary functions:

The Board functions as a mechanism for joint programming and procurement, with responsibilities that include helping the Commission identify priority funding areas that align with defence capability objectives established collectively by Member States under the Common Foreign and Security Policy (CFSP) framework, particularly those outlined in the Capability Development Plan [Art. 57(3)].

It supports EDIP implementation with a particular focus on crisis response and supply chain security through: analysing crisis-relevant information [Art. 57(5a)], assessing crisis state activation criteria [Art. 57(5b)], providing guidance on crisis response implementation [Art. 57(5c)], and facilitating information exchange with other crisis-relevant bodies [Art. 57(5e)]. These crisis response functions of the Board are directly tied to the supply chain security measures (detailed in the section "Supply Chain Security" below), where the Board plays a crucial role in coordinating responses to both general supply disruptions and security-related supply crises.

The Regulation specifies a clearly defined institutional composition for the Board, including representatives from the Commission (which chairs the Board), the High Representative and European Defence Agency head, Member States, and associated countries [Art. 57(7)]. To ensure industry input, the Board must facilitate formal engagement by convening with National Defence Industrial Associations and selected industry representatives minimum once annually [Art. 57(10)].

While this represents an evolution in European defence coordination, its role is more precisely focused on specific functions rather than broad industrial policy-making. The Board operates as a structured coordination mechanism, particularly focused on supply chain resilience and crisis response, working within clearly defined parameters to support the broader objectives of EDIP.

Structure for European Armament Programme

A key institutional innovation introduced by the Regulation is the Structure for European Armament Programme (SEAP). Articles 22 to 24 establish SEAP's fundamental framework, which serves a dual purpose: fostering the competitiveness of both the European and Ukrainian defence industrial bases by aggregating demand for defence products throughout their lifecycle [Article 22(1)].

SEAP's operational scope encompasses three principal tasks:

- Common procurement, which extends beyond basic purchasing to include R&D, testing, certification, and initial production support,
- Joint lifecycle management, incorporating spare parts procurement, logistics services, and public-private partnerships to maximize defence product availability,
- Dynamic availability management through a Defence Industrial Readiness Pool, ensuring participating states have immediate and preferential access to additional quantities through purchase or lease options [Article 22(2)].

The SEAP establishment requirements (Article 23) ensure broad participation while maintaining EU centrality: while a SEAP can be established by three participants, including associated countries or Ukraine, it must include at least two EU Member States. Importantly, each SEAP must align with capability priorities agreed upon under the Common Foreign and Security Policy framework and the Capability Development Plan [Article 23(1a)]. This alignment ensures that individual SEAPs contribute to broader European defence objectives.

To ensure operational effectiveness, SEAPs must follow standardized procedures and Commission guidelines for program management, funding, and reporting [Article 23(2)]. The application process (Article 24) requires detailed documentation including statutes and descriptions of defence equipment, technology, and services to be jointly procured and managed, with host Member States providing formal recognition of SEAP's international body status for tax (such as VAT and excise duty) and regulatory purposes.

The Regulation deliberately enables the creation of multiple SEAPs rather than establishing a single centralized structure. This flexible, multi-SEAP approach serves several strategic purposes:

First, it allows for a specialized focus on different capability areas. Since each SEAP must align with capability priorities under the Common Foreign and Security Policy framework [Article 23(1a)], different SEAPs can be established to address specific capability needs – for example, one focusing on air defence systems, another on ground systems, and yet another on maritime capabilities. This specialization enables more focused expertise and management of specific defence domains.

Second, the multi-SEAP structure provides flexibility in participation. While each SEAP requires at least two Member States, different groupings of Member States, associated countries, and Ukraine can form different SEAPs based on their specific defence priorities and industrial capabilities. This "variable geometry" approach allows for more agile cooperation configurations while maintaining the overall framework's coherence through standardized procedures and Commission guidance [Article 23(2)].

Third, this approach enables the parallel development of multiple defence capabilities while managing complexity. Rather than attempting to coordinate all joint defence procurement and lifecycle management through a single structure, multiple SEAPs can operate simultaneously, each with its own focused mandate but following common rules and procedures.

This architectural choice reflects a pragmatic balance between the need for coordination and the reality of diverse defence requirements and industrial capabilities across participating states. The Commission maintains overall coherence through its assessment and oversight role (Article 24) while allowing for the operational flexibility needed in complex defence procurement and management programs.

The Relationship Between the Board and SEAPs

The Regulation creates a clear division of responsibilities between the Defence Industrial Readiness Board and SEAPs. The Board functions as a strategic coordinator, identifying funding priorities and managing crisis responses at the system level. Meanwhile, SEAPs serve as operational tools for specific defence programs, handling the practical aspects of joint procurement and lifecycle management.

This arrangement works much like an orchestra, where the Board acts as the conductor, ensuring that all parts work together harmoniously, while individual SEAPs are the sections playing their specific parts. The Board's annual meetings with industry representatives help address broader issues affecting multiple programs, while SEAPs handle day-to-day relationships with contractors and suppliers for their specific projects. This structure is particularly important for integrating Ukraine's defence industry as it provides both high-level coordination through the Board and specific cooperation opportunities through participation in specific SEAPs (see the section "Ukraine's Industrial Integration" below for a comprehensive analysis of the Ukrainian defence industrial integration framework).

Supply Chain Security

The EDIP regulation introduces a comprehensive set of supply chain security measures that reflect the EU's growing focus on securing critical defence capabilities. These measures are structured across multiple layers, from monitoring and prevention to crisis response, creating an integrated approach to supply chain resilience.

At the foundation of these measures lies a sophisticated mapping and monitoring system. Article 40 of the Regulation mandates the Commission to conduct detailed mapping of the Union's defence supply chains, working in partnership with the Defence Industrial Readiness Board, which prepares a list of key defence products. This mapping exercise goes beyond simple documentation – it requires the identification of key defence products critical for security and defence interests. The process includes developing a framework for identifying crisis-relevant products and their related manufacturing capacities, with particular attention to potential bottlenecks that could disrupt supply chains.

The Regulation establishes a proactive monitoring framework through Article 41, which requires regular surveillance of manufacturing capacities necessary for crisis-relevant products. This monitoring system is notable for its multi-faceted approach, incorporating early warning indicators, Member State oversight of key market activities, and the identification of best practices for risk mitigation. To ensure effectiveness while minimizing bureaucratic burden, the Regulation specifically considers the impact on SMEs and includes provisions to streamline information collection from these smaller enterprises.

A particularly innovative aspect of the supply chain security framework is the creation of two distinct crisis response mechanisms. The first, detailed in Articles 43–47, addresses supply crises affecting the broader economy[18] that impact defence production. The second, outlined in Articles 48–54, deals with security-related supply crises directly affecting defence capabilities.[19] These mechanisms include powerful tools such as priority-rated orders, which can require companies to prioritize certain defence-related productions, and information-gathering powers that help authorities understand and address supply chain disruptions.

The Regulation also introduces practical measures to accelerate supply chain responsiveness. Article 38 requires Member States to ensure that administrative applications related to defence production facilities and product certification are processed efficiently. This is complemented by Article 39's provisions for easing cross-certification processes, which include the creation of an official list of national certification authorities and frameworks for information sharing among these bodies.

To ensure compliance and effectiveness, the Regulation includes enforcement mechanisms through Article 55, which establishes penalties for non-compliance with information requests or fulfilling priority-rated orders (a failure to accept or prioritize production of crisis-relevant non-defence products). These penalties are carefully calibrated, with different levels of fines based on the severity and nature of the violation, and special consideration for SMEs.

Perhaps most importantly, the Regulation creates a framework for preventive action through Article 43, which establishes an alert system for potential supply chain disruptions. This system allows for early intervention when risks are identified, enabling coordinated responses before full-scale crises develop. The Defence Industrial Readiness Board plays a crucial role here, coordinating responses and facilitating dialogue among stakeholders to address emerging challenges.

[18] Note: non-defence products needed for defence production, repair, maintenance, etc.

[19] Note: serious disruptions in the provision/trade of defence products or related intermediate products or raw or processed materials.

Industrial Strengthening Measures

One of the most significant aspects of this industrial strengthening approach is its focus on the entire industrial ecosystem. The Regulation recognizes that a strong defence industrial base requires not just major manufacturers but also a robust network of suppliers, particularly SMEs. This is reflected in various provisions throughout the Regulation, including specific support measures for smaller companies to obtain necessary quality and production certifications.

Central to this industrial strengthening effort is the Fund to Accelerate Defence Supply Chain Transformation (FAST), established under Article 19. This innovative financial mechanism is specifically designed to address one of the most pressing challenges in the defence sector – the need to support smaller players in the industrial ecosystem. FAST aims to leverage, de-risk, and accelerate investments needed to increase the defence manufacturing capacities of SMEs and small mid-caps. The fund operates through blending operations, offering debt and equity support and creating a multiplier effect that helps attract both public and private sector financing.

The Regulation places particular emphasis on manufacturing capacity enhancement through Article 11(3), which outlines "industry reinforcement actions". These actions encompass a broad range of initiatives, from optimizing and modernizing existing production facilities to establishing entirely new ones. The Regulation specifically allows for the establishment of cross-border industrial partnerships, including public-private partnerships, recognizing that international collaboration is key to building a more integrated European defence industry.

A particularly innovative aspect of the industrial strengthening framework is the concept of "ever-warm facilities"[20] – reserved surge manufacturing capacities that can be activated when needed. This approach, detailed in Article 11(3c), ensures that the European defence industry maintains the ability to rapidly scale up production in response to emerging needs while managing the economic challenges of maintaining excess capacity.

The Regulation also addresses the critical issue of industrial readiness through the creation of a Defence Industrial Readiness Pool, outlined in Article 14. This mechanism serves multiple purposes: it increases the availability of EU-made defence products, speeds up delivery times, and ensures preferential purchase options for Member States and Ukraine. The pool concept represents a practical solution to the challenge of maintaining industrial capabilities while managing procurement efficiency.

The industrial strengthening framework also includes specific measures to support innovation and technological advancement. Article 52 provides for emergency defence innovation actions, allowing for rapid adaptation of civilian products for defence applications and the significant shortening of delivery lead times. This flexibility is crucial for maintaining industrial competitiveness and responsiveness to evolving security needs.

[20] Note: "Ever-warm" in this context refers to maintaining production facilities in a ready state – not fully active but capable of quickly ramping up production when needed. It is between "cold" (shut down) and "hot" (fully operational) capacity, keeping essential systems and capabilities maintained for rapid activation.

Ukraine’s Industrial Integration

The EDIP regulation establishes a comprehensive framework for supporting and modernizing Ukraine’s defence industrial capabilities, apparently acknowledging the strategic importance of integrating Ukraine’s Defence Technological and Industrial Base (Ukrainian DTIB) with European defence structures. This support is woven throughout the Regulation but finds its clearest expression in the dedicated Ukraine Support Instrument (USI) established in Article 1(2) of the Regulation.

The Regulation’s approach to Ukrainian defence industry support is guided by a strategic vision outlined in Article 4. This vision encompasses not just immediate support but looks ahead to Ukraine’s potential future integration into the European defence industrial landscape. The Regulation specifically emphasizes that actions supporting Ukraine’s defence industry should take into account its possible future integration into the EDTIB, thereby contributing to mutual stability, security, and sustainability.

A particularly significant aspect of this support framework is found in Article 21, which establishes specific eligibility criteria for legal entities involved in Ukrainian defence projects. The Regulation creates flexible yet secure pathways for cooperation, allowing recipients of Union funding to be established either in the EU or in Ukraine. This provision is carefully balanced with security considerations. While entities can use infrastructure and facilities outside the EU or Ukraine when necessary, such use must not compromise security interests and must align with the Regulation’s broader objectives.

The financial architecture supporting Ukrainian defence industry development is addressed through several mechanisms. Article 5(1b) provides for dedicated funding through additional contributions, subject to specific agreements outlined in Article 59. This funding structure is designed to be both flexible and sustainable, allowing for various forms of support ranging from direct industrial modernization to joint procurement initiatives.

The Regulation facilitates practical cooperation through several mechanisms. Articles 22–24 explicitly include Ukraine as a potential participant in SEAPs, enabling Ukrainian defence manufacturers to participate in joint procurement and lifecycle management programs. Additionally, under Article 22(2c), Ukraine has access to the Defence Industrial Readiness Pool mechanism, allowing for immediate and preferential purchase or lease options alongside Member States and associated countries.

The Regulation places particular emphasis on modernizing Ukrainian defence facilities to NATO standards, as indicated in Article 4(5). This includes provisions for creating or expanding manufacturing capacities, protecting assets, enabling technical assistance, and facilitating personnel exchanges. The Regulation also promotes increased cooperation in the common procurement of defence products for Ukraine and encourages licensing production cooperation through various forms, including public-private partnerships and joint ventures.

To ensure effective implementation, Article 59 mandates the establishment of an EU–Ukraine Framework agreement. This agreement sets out detailed provisions for implementing actions involving Ukraine or Ukrainian entities receiving Union funds. It includes specific requirements for monitoring, control, and audit procedures, while also ensuring appropriate protection of classified information and adherence to security standards.

This comprehensive support framework reflects a strategic mindset that strengthening Ukraine’s defence industrial capabilities serves both immediate practical needs and longer-term strategic goals for European security architecture. The Regulation creates multiple pathways for cooperation while maintaining necessary safeguards and oversight mechanisms, establishing a foundation for the sustained development of Ukraine's defence industrial capabilities in line with European standards and practices.

STRATEGIC IMPLICATIONS AND FUTURE PROSPECTS

Strategic Implications

Beyond the Defence Industrial Readiness Board discussed previously, the Regulation's approach to supply chain resilience represents another crucial strategic implication.

The mapping and monitoring mechanisms established in Articles 40 and 41 go beyond simple industry oversight – they create a comprehensive understanding of European defence industrial capabilities and vulnerabilities. This knowledge base enables strategic decision-making about where to invest and how to protect critical capabilities. It is particularly significant that the Regulation includes provisions for early warning systems [Article 40(8)] and crisis response mechanisms (Art. 43, 44, 47, 48, 50), indicating a strategic shift towards anticipatory rather than reactive policy-making.

The Regulation also has important implications for Europe's international defence relationships. While strengthening European industrial autonomy, it creates frameworks for controlled cooperation with non-EU partners through carefully structured eligibility criteria (Article 10) and third-country participation rules. This balanced approach suggests a strategic vision of "open strategic autonomy",[21] meaning maintaining European independence while avoiding harmful isolation.

Perhaps most significantly, the Regulation's provisions for supporting Ukraine's defence industry (Chapter II, Section 3) indicate a strategic vision of an expanded European defence industrial space. This approach suggests a longer-term strategic goal of integrating neighbouring partners into European defence industrial networks, potentially creating a broader security architecture beyond current EU boundaries.

These strategic implications demonstrate how the EDIP represents not just a funding program but also a comprehensive attempt to reshape European defence industrial policy for long-term strategic advantage.

Future Outlook and Implementation Challenges

These strategic implications point towards EDIP's longer-term transformative potential. The European Defence Industry Programme represents an ambitious attempt to transform the EU defence industrial policy, with implications extending well beyond its initial 2025–2027 timeframe. The Regulation's comprehensive supply chain security framework, established through Articles 40–54, could evolve into a permanent system for managing the European defence industrial capacity. This framework, combining sophisticated mapping

[21] Note: As the European Parliament think tank puts it, "Open Strategic Autonomy ensures the capacity to cope alone if necessary but without ruling out cooperation whenever possible." https://www.europarl.europa.eu/thinktank/en/events/details/the-future-of-eu-s-open-strategic-autono/20230215WKS04981

mechanisms (Article 40) with two distinct crisis response tools (Articles 43–47 and 48–54), may serve as a model for addressing long-standing issues of fragmentation in European defence markets.

The SEAP framework, detailed in Articles 22–33, has particular potential for future development. The Regulation's deliberate choice to enable multiple specialized SEAPs, rather than a single centralized structure, creates flexibility for evolution in different capability domains. As outlined in Article 22(2), each SEAP can focus on specific areas while maintaining alignment with Common Foreign and Security Policy priorities. This approach, combined with innovative concepts like "ever-warm" facilities [Article 11(3c)], could establish new patterns of sustained industrial cooperation.

The Regulation's approach to Ukrainian defence industrial integration, anchored in Article 4(5) and detailed throughout Chapter II, Section 3, may establish a template for future defence industrial cooperation with EU candidate countries. The comprehensive framework created through Articles 21 and 59, addressing everything from eligibility criteria to security requirements, could guide similar integration efforts. This aligns with the EU's security commitments to Ukraine, specifically calling for "foster[ing] greater cooperation between their defence industries in the spirit of the European Defence Industrial Strategy".[22]

However, successful implementation faces several challenges. As outlined in Articles 10, 21, and 59, effective integration requires robust security frameworks for protecting classified information and controlling access to sensitive technologies. The Defence Industrial Readiness Board's effectiveness will depend on successful coordination among EU institutions, Member States, and industry representatives. Regular industry engagement through what the Regulation terms "structured dialogue" [Article 57(10)] will be crucial for adapting to new regulatory requirements and crisis response mechanisms.

As the proposal is currently under discussion in both the European Parliament and Council, the final shape of these mechanisms may evolve through the legislative process. However, the fundamental approach of creating permanent structures while maintaining flexibility appears likely to remain central to the Regulation's design.

In brief, the Regulation's strategic vision emerges primarily through its comprehensive approach to strengthening European defence industrial capabilities. Its supply chain security framework (Articles 40–54) establishes unprecedented monitoring and crisis response tools, while the SEAP mechanism (Articles 22–33) creates flexible structures for defence industrial cooperation. This foundation is complemented by carefully structured frameworks for international partnerships, particularly with Ukraine. This combination, overseen by the Defence Industrial Readiness Board (Article 57), marks a fundamental shift from voluntary coordination to the active management of defence industrial capabilities. As EDIP bridges the gap between current emergency measures like ASAP and EDIRPA (expiring in 2025) and future long-term initiatives, its success in establishing these permanent structures will likely shape the design of the EU defence industrial policy under subsequent Multiannual Financial Frameworks.

[22] EU-UKR 2024.

CONCLUSIONS

The European Defence Industry Programme (EDIP) represents a fundamental transformation of the EU defence industrial policy, moving beyond temporary crisis responses towards a comprehensive framework for long-term industrial readiness. While its €1.5 billion funding envelope for 2025–2027 remains modest, the Regulation's significance lies in its innovative institutional and regulatory mechanisms that create permanent structures for European defence industrial cooperation.

The Regulation introduces several transformative elements that together mark a shift from voluntary coordination to the active management of defence industrial capabilities. At its core, the Structure for European Armament Programme (SEAP) framework creates flexible arrangements for joint procurement and lifecycle management, allowing specialized programs to develop in parallel while maintaining strategic coherence. This is complemented by a sophisticated supply chain security system that combines preventive monitoring with powerful crisis response tools, including unprecedented powers for priority-rated orders and emergency innovation support.

The Regulation's approach to industrial strengthening reflects a mature understanding of the defence industrial ecosystem. Through mechanisms like the Fund to Accelerate Defence Supply Chain Transformation (FAST) and the innovative "ever-warm" facilities concept, it addresses both immediate production needs and long-term industrial resilience. The Defence Industrial Readiness Board (DIRB) provides strategic coordination across these various elements, ensuring that individual initiatives contribute to broader European defence objectives.

While primarily focused on strengthening European capabilities, the Regulation also creates carefully structured frameworks for international cooperation, particularly through its comprehensive approach to Ukrainian defence industrial integration. This balance between internal capability building and strategic partnerships reflects a pragmatic approach to achieving greater European defence industrial autonomy.

Looking ahead, EDIP's effectiveness will depend on the successful implementation of its various mechanisms, particularly the coordination among EU institutions, Member States, and industry through the Board's "structured dialogue". However, by establishing permanent structures for defence industrial cooperation while maintaining operational flexibility, EDIP creates a foundation for more integrated European defence industrial development that will likely shape policy evolution well beyond its initial timeframe.

BIBLIOGRAPHY

- BLOOMBERG[@business]: *The problem is not Trump or the US, the problem is Europe.* Twitter, 23 January 2025. https://x.com/business/status/1882375864777605342 (Downloaded: 01/02/2025).
- European Commission: *EDIRPA Addressing Capability Gaps*. European Commission Website, 2023. https://defence-industry-space.ec.europa.eu/eu-defence-industry/edirpa-addressing-capability-gaps_en (Downloaded: 01/02/2025).
- European Commission: *European Defence Fund (EDF)*. Commission Website, 2025. https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en (Downloaded: 01/02/2025).

- European Commission: *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A new European Defence Industrial Strategy: Achieving EU readiness through a responsive and resilient European Defence Industry*. European Commission Policy Document, JOIN(2024) 10 final, 5 March 2024. https://defence-industry-space.ec.europa.eu/document/download/643c4a00-0da9-4768-83cd-a5628f5c3063_en?filename=EDIS%20Joint%20Communication.pdf (Downloaded: 01/02/2025).
- European Commission: *Proposal for a Regulation of the European Parliament and of the Council on Establishing the European Defence Industry Development Programme and a framework of measures to ensure the timely availability and supply of defence products ('EDIP')*. European Commission Legislative Proposal, COM(2024) 150 final, 5 March 2024. https://defence-industry-space.ec.europa.eu/document/download/6cd3b158-d11a-4ac4-8298-91491e5fa424_en?filename=EDIP%20Proposal%20for%20a%20Regulation.pdf (Downloaded: 01/02/2025).
- European Commission: *Staff Working Document for a European Defence Industry Programme and a framework of measures to ensure the timely availability and supply of defence products*. 8 July 2024. https://defence-industry-space.ec.europa.eu/document/download/f1e6ba44-4720-4f14-a991-a3a7f3afb475_en?filename=Staff%20Working%20Document%20on%20EDIP.PDF (Downloaded: 01/02/2025).
- European Commission*: The Commission allocates €500 million to ramp up ammunition production, out of a total of €2 billion to strengthen EU's defence industry*. European Commission Press Release, 15 March 2024. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1495 (Downloaded: 01/02/2025).
- European Defence Agency: *European Defence Fund (EDF)*. Agency Website, 2025. https://eda.europa.eu/what-we-do/EU-defence-initiatives/european-defence-fund-(edf) (Downloaded: 01/02/2025).
- European Union and Ukraine: *Joint security commitments between the European Union and Ukraine*. Agreement Document, 27 June 2024. https://www.consilium.europa.eu/media/oredhmis/eu-ukraine-security-commitments-en.pdf (Downloaded: 01/02/2025).
- Hunnicutt, Trevor: *Trump says he is not sure US should be spending anything on NATO*. Reuters News Article, 24 January 2025. https://www.reuters.com/world/us/trump-says-not-sure-us-should-be-spending-anything-nato-2025-01-23/ (Downloaded: 01/02/2025).
- Kayali, Laura: *As Trump arrives, Macron hints NATO spending target is too low*. POLITICO, 20 January 2025. https://www.politico.eu/article/france-emmanuel-macron-hints-nato-spending-target-is-too-low-donald-trump/ (Downloaded: 01/02/2025).
- *Regulation (EU) 2023/1525 of the European Parliament and of the Council of 20 July 2023 on supporting ammunition production (ASAP)*. Official Journal of the European Union, L 185/7. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1525 (Downloaded: 01/02/2025).

Ferenc Tampu

OSINT[1] BEYOND SECURITY POLICY

DOI: 10.35926/HDR.2025.1.4

ABSTRACT: *The objective of the paper is to give a brief overview of OSINT, which was originally used mainly in military operations in the field of state security intelligence, in light of the literature. First, the concept of information is clarified by illuminating it with concise definitions. Foreign and domestic approaches to the subject are compared in a few words. Some historical examples are given to illustrate OSINT's use in the past and its application in different fields and periods. The importance of OSINT extends beyond its everyday use, as evidenced by the fact that it is still used today by governmental bodies, in security policy, from the civilian sector to marketing. The World Wide Web and social media have brought radical changes. They have transformed the way we search for information and the tools we use. At the same time, the development of information technology has seen unprecedented progress. This is why both computers and artificial intelligence have been put at the service of open-source intelligence. The paper considers both the advantages and disadvantages of OSINT and reflects on legal and ethical issues, providing a background knowledge of the law.*

KEYWORDS: *OSINT, open-source intelligence, information, military intelligence*

ABOUT THE AUTHOR:

Ferenc Tampu is a librarian and information scientist at Semmelweis University, Faculty of Health Sciences. He graduated from the Library and Information Science MA and History Teacher MA at Eötvös Loránd University (MTMT: 10097484).

INTRODUCTION

From the very beginning, information has been essential for humanity because it meant knowledge – and knowledge is power. Already in ancient times, it was collected and used to its advantage. Over the centuries, the methods and means of collecting information have evolved and changed. Open-source intelligence, commonly known as OSINT, has thus become one of the most widely used methods because it is cost-effective, accessible to all, legally obtainable, and, within certain limits, ethical. Since the Middle Ages, it has become an indispensable tool for state institutions, both at the military and decision-making levels. At that time, libraries were one of the main sources of freely available information. The development of information technology in the 20th century led to a wider dissemination of OSINT. The real turning point came with the advent of the Internet, which increased the volume and speed of OSINT, as well as its methods to an unimaginable extent. The focus shifted from traditional sources to virtual sources that could be accessed and obtained over the Web. It has thus become one of the most topical and rapidly evolving academic fields of

[1] Open Source Intelligence.

our time. It is now used by all disciplines, from public intelligence organizations to civilian society and the corporate and commercial sectors. The questions are: despite its advantages, disadvantages, and dangers, to what extent do we use OSINT consciously in our everyday lives, and is the general perception true that the Web has completely taken over the role of the library as an information center? My study aims to examine, analyze, and clarify the use, evolution, and development of open access to information in different eras. I do not aim to be exhaustive in such a topical field, but provide a few mosaic-like cases, ideas, and analyses that may inspire a deeper understanding and research of the process used today.

INFORMATION

It is perhaps worth starting with the essence of the topic: to clarify the concept of information in a few sentences, without claiming completeness, since the core of OSINT is information itself. Since the beginning of mankind, information has played an important role in all areas of life. Although at first sight it seems a simple concept,[2] if we go deeper, we find ourselves in a jungle of inextricable meanings. For just as the various disciplines have diverged over time, so has information science taken its place in the system. There is now a huge body of literature on it, a plethora of definitions,[3] and different aspects of different disciplines have different perspectives.[4] Therefore, all disciplines from applied sciences to social sciences have developed a world of meanings for information. This is how, among other things, mathematical information theory and social science theory were born, but the economic and philosophical approaches are also well known.[5]

Far from being exhaustive, a few basic definitions of information are given here to underline its importance: "Information is observation, experience, or knowledge given in an accessible form about certain facts, objects, or phenomena […] The concept of information is closely related to the concepts of data and knowledge […] Information is interpreted data, that is, the subjective meaning of data for a person or organization […] In the digital age, the production, use, management, and spread of information have been given a prominent role […] Information is a special resource".[6]

Going beyond theoretical approaches, we know that throughout history, information has been of inescapable practical importance, a source of power, and often an impregnable advantage over adversaries. Information and its possession were simply indispensable during the various small-scale or major wars.

Information also brings many benefits and advantages in achieving peaceful goals in times of peace, if it is accessed first and at the right time. In the civil and economic spheres, in commerce, in the corporate sector, at the political level, and even in everyday life, information is a key to progress and advancement. First, knowing where and what is in demand is the most powerful weapon a trader or manufacturer has against its competitors. This brings us to one of the most important properties of information: the time factor. It is not enough to get the information; one must take the time to get it and use it in the right way at the right time. From the moment it is made public and more and more people possess it,

[2] Word of Latin origin: news, message, information.

[3] Vakkari – Cronin (eds.) 1992.

[4] Fülöp 1996.

[5] Capurro 1992.

[6] Orbán, no year.

its value exponentially decreases. It may sound cliché, but it is still true that information is the most useful if it is made public. The main cornerstone of this analysis is OSINT,[7] i.e., open-source intelligence that is freely available to all. Its importance and relevance are demonstrated by the fact that it has been gaining prominence in decision-making at the government level for decades. Public authorities around the world, including our own, place increasing emphasis on open-source information. This is reflected in the various bodies that have been set up for decades to deal with open-source intelligence. Just to look back over the last quarter of a century, in Hungary between 2001 and 2016, this task was carried out by the Coordination Center Against Organized Crime (SZEBEKK), which was established by Act CXXVI of 2000.[8] As its successor, the Counter-Terrorism Information and Criminal Analysis Center (TIBEK) started its operation on 17 July 2016, in accordance with the 1995 Act on the Coordination Center Against Organized Crime. In 2022, the coordination of civilian national security services was unified, and the National Information Center (NIC) started to operate as the successor of the previous organizations.[9]

THE CONCEPT OF OSINT

Although there is no fixed definition, the concept of OSINT has been elucidated in various forms by several authors. In fact, at the turn of the millennium, NATO, one of the world's largest organizations, published a handbook in which it defined and clarified OSINT's essence and tools. "OSINT is information that has been deliberately discovered, discriminated, distilled, and disseminated to a *select* audience, generally the commander and their immediate staff, in order to address a *specific* question."[10] America's National Defense Authorization Act introduced a few years later, in 2006, also includes a definition of OSINT: "Open-source intelligence (OSINT) is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."[11]

To get a clearer picture of OSINT, look at some definitions from some Hungarian authors. Perhaps one of the most general definitions is from Péter Bányász: "Open-source intelligence retrieval […] is an information gathering process whereby information is retrieved from publicly available sources, analyzed, evaluated, and used for a specific purpose."[12] Another is from Gábor Lévay: "It refers to the professionally based search for, collection, selection, analysis, evaluation, and use of information that exists outside the military intelligence and reconnaissance system, which is publicly available (i.e., to all individuals) by legal means or is disseminated in a restricted circle, but is not classified".[13] A third researcher, Csaba Vida, defines the concept as follows: "OSINT activity: the autonomous open data collection activity means the search for, collection, selection, evaluation, and use of unclassified data, published by a person or organization, publicly available by lawful

[7] Today, there is an inexhaustible number of sources available, both printed and electronic.

[8] *2000. évi CXXVI. törvény a Szervezett Bűnözés Elleni Koordinációs Központról* (Act CXXVI of 2000 on the Coordination Center Against Organized Crime) 2000.

[9] Nemzeti Információs Központ (National Information Center) 2022.

[10] NATO 2001, 2–3.

[11] *PUBLIC LAW 109–163.*

[12] Bányász 2015, 23.

[13] Lévay 2006, 6.

means or disseminated in a restricted manner, based on a specific methodology, to meet intelligence needs".[14]

Among the plethora of definitions, the essential difference between the above is that while the US documents refer to open-source information as the object of intelligence gathering, Hungarian researchers emphasize not only the public quality of the source but also the open nature of the information itself. It follows that such information cannot be classified. In its simplest formulation, we speak of OSINT when the information is available to anyone in the public domain and can be obtained by legal means, including information that is distributed in a restricted way, thus, is subject to registration or subscription. Regardless of the type of OSINT (civil, military, or business intelligence), it has become part of our everyday lives, and everyone collects and uses it according to their own needs and requirements.[15] Its unity – and most of all its importance – is most evident from the fact that it is indispensable for certain procedures at almost all levels of management and is vital in decision-making.[16]

It should also be made clear that OSINT is not the same as surfing the Internet or gathering information from social media alone. It is an operation, a procedure that involves the collection, processing, interpretation-evaluation, and use of information according to certain criteria for a certain purpose. From the collection and processing of this information, it is possible to generate even classified information through analysis-evaluation by appropriate professionals and comparison with other (even classified) information. OSINT's main elements are therefore:

– data acquisition, which involves the collection of open information;
– processing the information (validation);
– evaluating, analyzing, and determining the usefulness of the information;
– compiling a report, transmitting it to the target audience or client.[17]

To summarize, the OSINT conceptual framework thus distinguishes between:

– OSINT activity;
– OSINT data;
– OSINT information;
– authenticated OSINT information.

Each has its own role and function in the system. OSINT activities include the search for and acquisition of publicly disclosed, unclassified information by lawful means, and its classification. OSINT data is such data that has not yet been published or processed by others, such as photographs, video recordings, letters, statements, etc. OSINT information is such information that has been selected according to certain criteria and gathered from open sources, such as books, newspapers, daily reports, etc. Certified OSINT information is such information that has been compared by experts and analysts to other information and facts, even from certified or verified sources, and declared reliable information based on this information.[18]

[14] Vida 2013.

[15] Solti 2019, 3.

[16] Szabó 2019, 69–71.

[17] Kis-Benedek 2020.

[18] Szabadföldi 2022, 38.

Today, in the world of the Internet, we tend to see the World Wide Web as the source, or at least the primary source, of OSINT. While it is true that with its emergence, an inexhaustible amount of information is available, growing exponentially every day, we cannot ignore the fact that its traditional sources are as useful today as they were in the past. Accordingly, the NATO Handbook (2001) identifies the following sources as the primary ones for OSINT:[19]

– traditional media sources (including both printed and digital);
– commercial online sources (both printed and digital);
– other forms of commercial online information;
– "grey literature" (non-public);
– overt human experts and observers;
– commercial imagery;
– commercial cameras;
– non-governmental organizations;
– religious organizations.

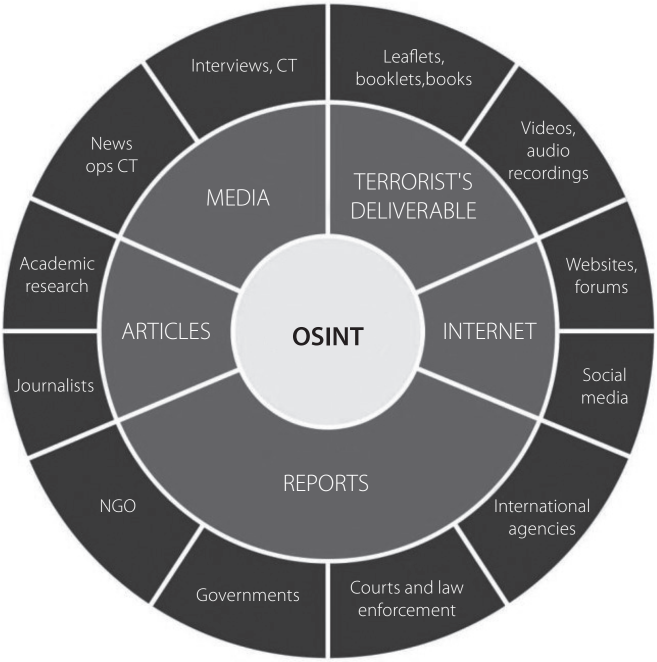


Figure 1 *OSINT and its sources*

Source: *https://linkurious.com/blog/graph-based-intelligence-analysis/*

In addition to these, Hungarian researchers add further sources to the above list. These include, for example, educational institutions, research institutions and their libraries, journalists, language schools, business and international organizations (e.g., the International Red Cross, the UN, and its various related organizations), and NGO briefings (hearings,

[19] NATO 2001, 5–11.

legislative debates, press conferences, and even the budget itself). Also, social networking sites on the Internet[20] and any platform or individual (e.g., data broker) that creates, provides, or contains information for the public.

OSINT IN THE PAST

OSINT, as an information gathering technique, is not new; its origins go back to antiquity, and it is practically as old as mankind. The devastating outcome of the famous Battle of Kadesh of the Egyptian Pharaoh Ramses II proves that not only information but also disinformation is crucial for those who use it well.[21] The advent of writing, the printed press, and the spread of books made it easier to collect, store, and categorize information, and more importantly, provided the news and information "divers" with significant source materials. Travelogues, narratives, chronicles, and war memoirs were the first OSINT sources. From a political point of view, the monitoring of the print media (daily newspapers, trade journals) was of particular importance. This is best symbolized by the 19th-century saying attributed to British Prime Minister Lord Palmerston:[22] "We don't need spies, we read the Times".[23]

Returning to the operations, one of the indispensable aids was the map, which helped the troops to move. The most widely used maps were the Michelin company's road maps, which were commonly used in the Second World War, both in North Africa and during the advance in Italy and France. Guidebooks and various briefing books were also a great help as OSINT sources to diplomats, soldiers transferred to foreign countries, and secret agents. The range of OSINT sources continued to expand with the development of technology. Thus, the advent of telecommunications and radio broadcasting further enriched the range of OSINT tools.[24]

The emergence of the terminology used today (OSINT) itself is not related to the spread of the Internet; it dates back much earlier. Its first traces can be found primarily at the political level, where the method of searching for information to support decisions was already in use before the mid-20th century. Its roots can most probably be traced back to America in the early 1940s. Based on research at Princeton University, President Roosevelt set up a financial fund to create a department (Foreign Broadcast Monitoring Service, FBMS) within the Federal Communications Commission to monitor and follow news and events in the foreign press and media and to inform the relevant government leaders. Eventually, this organization was integrated into the Central Intelligence Agency (CIA). In the half century that followed, OSINT underwent a major evolution and transformation.[25] Today, the use of open-source information is essential for decision-making in political and public issues, as well as for effective national security.

The real breakthrough for OSINT has been the emergence and explosion of the Internet and digital networks. At the same time, the exponential growth of data on the web has made it possible to obtain information rapidly through digital means, making open-source

[20] Kis-Benedek 2020.

[21] Dezső 2019, 18.

[22] British Foreign Secretary 1830–1841 and 1846–1851 and Prime Minister 1855–1865.

[23] Regényi 2019, 33.

[24] Regényi 2019, 34.

[25] Márton 2023, 1424.

intelligence an increasingly dynamic industry.[26] The emergence of the World Wide Web has therefore led to an explosion of information. At the same time, storage capacities are also increasing and becoming more affordable.[27]

Social media itself has brought further changes to OSINT. Its emergence and increasing use, which started more than two decades ago, have brought new opportunities. In the words of Eszter Vattai, "Social media is a goldmine of open-source information acquisition".[28] The more a person uses the Internet, including social media, the more information can be gathered about them.

Social media, especially through video-sharing portals, are increasingly playing an opinion-forming role. Thanks to their sharing functions, they can deliver their content to larger audiences, making them an excellent tool for influencing. From fashion to everyday habits, social and political events and news are being broadcast to an ever-wider audience and are nowadays consumed in a way that goes beyond television and radio broadcasting. At the same time, social media has also brought new challenges for OSINT users. One very serious challenge, for example, is the issue of disinformation.[29] Users often share information and data that is not true. In such cases, the veracity of this information must be checked from several sources. This is true not only for social media. History has repeatedly shown that the credibility of information gathered from various sources needs to be carefully assessed and checked to see whether it is reliable (see the Battle of Kadesh). This is particularly important in conflict situations. In such cases, it is impossible to establish their authenticity by relying on a single source. A very good example of this is the case in World War II, when German scientists used the timbre of the Big Ben bell to deduce the weather conditions, which was important for planning the bombing of the city and choosing the time of the bombing. Finally, when the British realized this, they began to broadcast the bell's chime from a recording, thus deceiving the enemy.[30] A similar disinformation was reported in the early 19th century, when Napoleon and Admiral Nelson, in their battles, published inaccurate information about the numbers, equipment, and positions of the Toulon army in Le Moniteur.[31] A series of examples from military history shows that disinformation can do as much harm to the enemy as the benefits gained from having the information.

Economists and commercial actors also take advantage of the benefits of OSINT daily. With the rise of social media, they can use the web to gather the most up-to-date information for their company. From consumer habits through trend analysis to information on competitors, all the most recent and relevant information can be gathered. The development of OSINT's business-to-business solutions is now a separate and growing market segment that can collect the most basic data on a global scale, especially using social media (see the trend analysis mentioned above), as it gives insight into our lifestyles, interests, and habits.[32] To this end, larger companies even use the services of data brokers, as they usually have the information technology tools needed to gather the most up-to-date and relevant information in a specific field.

[26] Molnár 2021, 84.

[27] Csizner 2019, 20–21.

[28] Vattai 2023, 159.

[29] Szabó 2019, 77.

[30] Csizner 2019, 19–20.

[31] Keegan 2005.

[32] Dobák 2019, 88.

OSINT AND ARTIFICIAL INTELLIGENCE (AI)

To begin with, the changing, accelerating, and ever-increasing flow of available information and its management, processing, and analysis are nowadays major challenges from a technical point of view. Therefore, the application of artificial intelligence in the context of OSINT cannot be ignored. Given the well-known and exponentially increasing information dumping (especially thanks to the World Wide Web) in recent years, it is no exaggeration to say that it is almost impossible to find and extract the most relevant and credible information in any field of expertise by human effort. To illustrate: 500 hours of video were uploaded per minute to YouTube in 2024 (roughly 2500 new videos) and 3.7 million videos per day. Also, 694,000 hours of video content were streamed by users every minute, which translates to 5 billion videos streamed per day. According to YouTube statistics, the site has around 2.67 billion users worldwide today.[33] The graph below illustrates how the number of users of this social media platform grew between 2010 and 2023.[34]

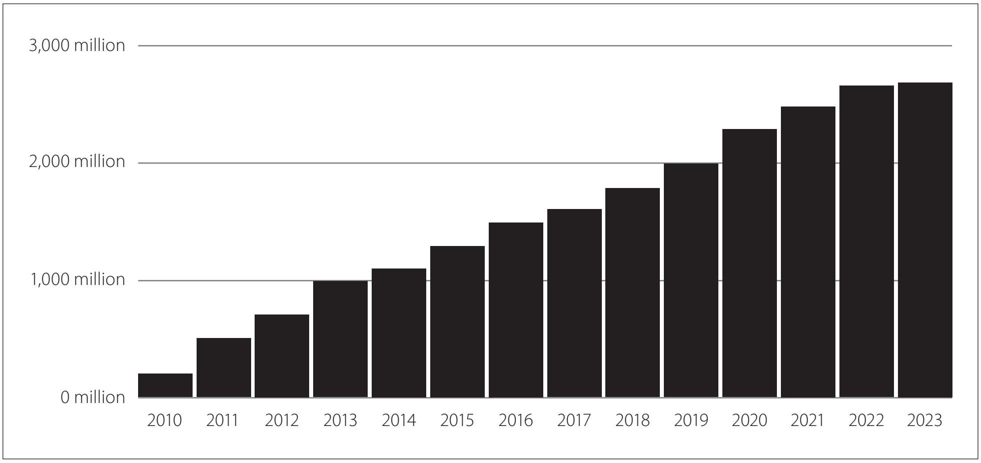


Figure 2 *YouTube users 2010–2023*

Not to mention that monitoring social media is almost impossible without the help of programs and software. Thus, the interaction between OSINT and AI is implemented through platforms and frameworks. Machine learning algorithms help to increase performance and speed. AI-enabled OSINT is also useful in information security, it is particularly effective for law enforcement, cyber threats, digital evidence collection, data leakage, etc. But the main goal of automating OSINT is to achieve as much performance as possible. It must be kept in mind that automated analysis of data cannot fully replace the need for human judgment.[35] The increased demand for open information has thus professionalized OSINT activities. A good example of this is the emergence of data brokers, who have perfected it through a variety of solutions, such as internet-based data collection methods and software development. It can therefore be seen that the ever more widespread

[33] Péter 2024.

[34] Shaw 2025.

[35] Szabadföldi 2022, 42.

use of OSINT anticipates the development of the information technology environment, the gradual application of artificial intelligence, and the emergence and spread of specific forms of data and text mining technologies.[36]

BENEFITS OF OSINT

In addition to its undisputed usefulness, OSINT has several advantages. These are not insignificant to list:

- cost-effective, efficient acquisition of information;
- providing a comprehensive (global) and real-time overview;
- allowing users to monitor and obtain a significant part of foreign affairs intelligence on a daily basis;
- providing summaries, in-depth analyses, economic trends, and risk analyses;
- OSINT activities carried out in compliance with the rules are completely risk-free;
- can be run from home if the necessary organizational structure is put in place;
- rapid response capability;
- no need for permits, thus avoiding bureaucratic red tape.[37]

The first point, cost-effectiveness, certainly deserves some elaboration to get a clearer picture. According to the literature, for example, while intelligence agencies can obtain 80% of their information with 5% of their information acquisition costs using OSINT tools, the remaining 20% of information is gathered by other intelligence branches,[38] which consume 95% of their budget.[39] This is confirmed by Alan Dulles'[40] claim that the majority (80–90%) of intelligence information is open source.[41]

DISADVANTAGES OF OSINT

- Information abundance is disrupted. In today's information overload, it is often very difficult to filter out the most relevant information.
- Language difficulties: The content of information can be somewhat distorted in every translation. It is advisable to search primarily in the language of the country concerned.
- Protected data is difficult to access. This is, in fact, the essence of OSINT.
- There may be a lack of source checking and a need to check credibility, as there is a lot of incorrect, redundant, or even deliberately misleading information.
- Sometimes the information obtained may be one-sided or biased.
- Dispersion of open information: Most of the time, we do not even know if the information we are interested in exists, and if so, where to find it.[42]

[36] Dobák 2019, 90–91.

[37] Kis-Benedek 2020.

[38] HUMINT (Human Intelligence) = human operational activity, SIGINT (signal intelligence) = signal intelligence, technical intelligence, IMINT (imagery intelligence) = imagery intelligence, MASINT (Measurement and signature intelligence) = measurement intelligence.

[39] Szabadföldi 2022, 32.

[40] Former head of the CIA (Central Intelligence Agency) at the beginning of the Cold War.

[41] Regényi 2019, 34.

[42] Kis-Benedek 2020.

Beyond the advantages and disadvantages of OSINT, we may also encounter other limitations when using it. For example, there are legal, ethical, and even economic constraints. To comply with the legal limits, the CXXV Act of 1995[43] sets out the rules for data processing, authorizes service providers to process personal data, and sets out the ways of obtaining and further using the data. Other areas, such as marketing and market and scientific research, are guided by the 1992 Act[44] and the law known in the public domain as the General Data Protection Regulation (GDPR).[45]

Ethical issues include: can I store data and information (e.g., images, events, personal data) about individuals obtained from open sources for further use or analysis? This consequently leads back to the legal question.

We talk about economic limitations when we can only access certain content or databases by subscription, registration, or order. A technical barrier may exist if the acquisition and display of certain information requires an appropriate IT infrastructure, a special computer, software, or programs.

INTERNET VS. LIBRARY WHEN USING OSINT

Looking through a small (but from a professional point of view, the most current and scientific) part of the Hungarian literature, we can see that man's hunger for information has led to the emergence, development, and, say, triumph of OSINT. In the pre-Internet era, there were fewer threats to individuals, although there may have been to some sources. However, the World Wide Web has radically changed the way open-source information is available to all.

Connected to OSINT, but still slightly diverging from it, it would be very important to examine and compare the evolution and role of the use of libraries and the Web in this context. As we know, before the Internet, libraries and archives were the primary repositories of so-called open information. However, with the advent of the Web, libraries are known to have gradually been relegated to the background as the main places to find information. There is, therefore, a general perception that the number of library users is declining. Even the most extreme predictions, that we are approaching the end of the Gutenberg Galaxy,[46, 47] seem to be dissipating, as the usefulness of libraries and their role in science, research, and culture remain almost unchanged. So is their role as open repositories of information. However, it should be noted and accepted that the number of users (at the very least, the number of on-site users) has dwindled considerably, but by no means to the tragic extent that was predicted. And the demise of the book and library is no longer worth talking about. This leads to another hypothesis and question: Internet vs. library. In other words, in the case of open access to information, where do users primarily turn: to the Internet or the library? Before we quickly name the Web, let us be clear: the library can be used as a cross-platform on the

[43] *1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról* (Act CXXV of 1995 on National Security Services), 1995.

[44] *1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról* (Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Data of Public Interest), 1992.

[45] European Parliament and the Council 2016.

[46] The term Gutenberg galaxy refers to a period in human cultural history in which the printed book has been prominent as a medium of communication from the 15th century to the present day.

[47] Bujdosóné Dani 2012.

Web. So, let us distinguish between someone searching for information on the World Wide Web but not on a library platform, and searching in a library, whether they visit the library physically or via the Internet. After all, in the times when the Web started, libraries understood its triumphal march that continues to this day. They have adapted their activities and services to the opportunities offered by information technology and digitization, they have built up their digital infrastructure, and a large part of their collections are now available online. This is why libraries today are not just collecting documents, but also information. A significant part of their services is available online. The question is clear: where do we primarily look for information today, on the Web or in the library? It is particularly addressed to those who, even before the advent of the Web, had an information storage space, the library, as an integral part of their daily lives. These are students, teachers, and researchers in higher education and research institutions. It would be worthwhile and important to carry out this survey in the context of a larger-scale research project, which could answer the question, among others, as to what extent the use of OSINT, brought to the surface by the Internet and made part of everyday life, has made libraries self-conscious and marginalized them as open information-gathering and service institutions.

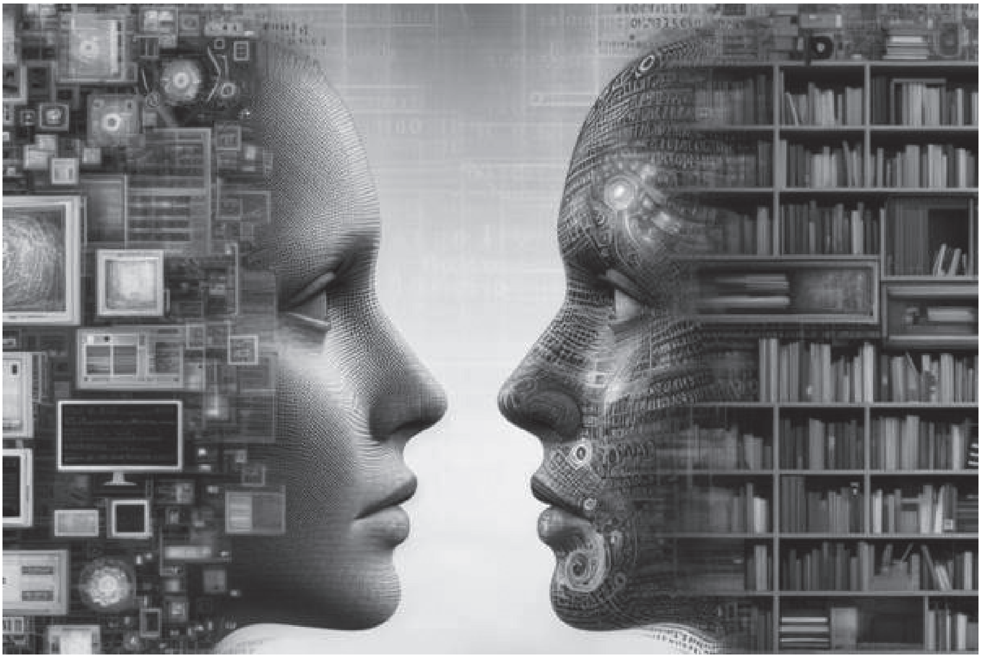


Figure 3 *Digital library vs. traditional library*

Source: *https://ic.softlinkint.com/blog/digital-library-vs-physical-library-the-ultimate-face-off/*

CONCLUSION

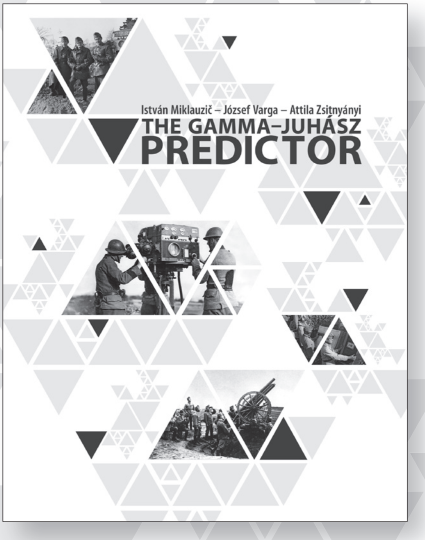
It is no exaggeration to say that OSINT, like any other field, has been characterised by evolution and continuous change. Its fundamental “cell”, information, has always determined its evolution. It has been used in different fields in different eras, its role being to satisfy mankind's hunger for information. Over time, it has played an increasingly important role in warfare and political decision-making, and public bodies have therefore provided an institutional framework for open-source information. In the 20th century, it became indispensable in law enforcement and the detection and prevention of terrorist acts. As we have seen, around 80% of intelligence information is obtained this way, also because of its cost-effectiveness. However, since the information explosion took place thanks to the Internet towards the end of the 20th century, civil, business, and corporate sectors now use it on their own devices, to their needs, and tastes. Trend analysis, habits, and competitor mapping are all areas where open access to information is now unthinkable. Social media has brought a new twist, where users create the content and the wealth of information, and the service provider only provides the framework. Nor can we ignore the fact that the increasing use of social media has been accompanied by the growing role of OSINT in shaping and influencing opinion. In particular, we can see – not only at home, but also abroad – how politics and different world views exploit this and try to use it to their own advantage. It is often easier to get information and news through social media (YouTube, Facebook, TikTok, X) than through traditional media (television, radio, newspapers, daily papers, etc.). Its advantages far outweigh its disadvantages, but this does not diminish its dangers, which should encourage everyone to use the Internet more consciously. It would be worthwhile to carry out a larger-scale study to find out how consciously OSINT is used in Hungary. It is at least as important a question whether the traditional information storage institutions (libraries and archives) have been replaced by the Web, as is now widely accepted as a fact, when collecting information by OSINT means.

BIBLIOGRAPHY

- *1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról* (Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Data of Public Interest), 1992. https://mkogy.jogtar.hu/jogszabaly?docid=99200063.TV (Downloaded: 13/01/2025).
- *1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról* (Act CXXV of 1995 on National Security Services), 1995. https://net.jogtar.hu/jogszabaly?docid=99500125.tv (Downloaded: 13/01/2025).
- *2000. évi CXXVI. törvény a Szervezett Bűnözés Elleni Koordinációs Központról* (Act CXXVI of 2000 on the Coordination Center Against Organized Crime), 2000. https://mkogy.jogtar.hu/jogszabaly?docid=a0000126.TV (Downloaded: 13/01/2025).
- Bányász, Péter: *A közösségi média, mint a nyílt forrású információszerzés fontos területe*. Nemzetbiztonsági Szemle, Vol. 3, No. 2 (2015), 21–36.
- Bujdosóné Dani, Erzsébet: *Neumann kontra Gutenberg-galaxis? – Különös tekintettel a generációs olvasási szokásokra*. Könyv és nevelés, Vol. 14, No. 4 (2012), 48–59.
- Capurro, Rafael: *What is information science for? A philosophical reflection*. In: Vakkari, Pertti – Cronin, Blaise (eds.): Conceptions of Library and Information Science: Historical, Empirical and Theoretical Perspectives. Taylor Graham, London, 1992, 82–98.
- Csizner, Zoltán: *Az OSINT határai*. Nemzetbiztonsági Szemle, Vol. 7, No. 2 (2019), 19–31. https://doi.org/10.32561/nsz.2019.2.2
- Dezső, Tamás: *Mezopotámia – Asszíria katonai felderítése*. In: Boda, József – Regényi, Kund (eds.): A hírszerzés története az ókortól napjainkig. Dialóg Campus Kiadó, Budapest, 2019, 18–22.

- Dobák, Imre: *OSINT – Gondolatok a kérdéskörhöz*. Nemzetbiztonsági Szemle, Vol. 7, No. 2 (2019), 83–93. https://doi.org/10.32561/nsz.2019.2.7
- European Parliament and the Council: *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. EUR-Lex, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC (Downloaded: 13/01/2025).
- Fülöp, Géza: *Az információ*. 2. bővített és átdolgozott kiadás, Eötwös Loránd Tudományegyetem Könyvtártudományi – Informatikai Tanszék, Budapest, 1996.
- Keegan, John: *A háborús felderítés*. Európa Könyvkiadó, Budapest, 2005.
- Kis-Benedek, József: *Az OSINT alkalmazása a diplomáciában*. In: Nagy, Sándor Gyula – Kutasi, Gábor (eds.): Gazdaságdiplomácia – Elmélet és gyakorlat felkészülő diplomatáknak. Akadémiai Kiadó, Budapest, 2020. https://mersz.hu/hivatkozas/m725gegyfd_244#m725gegyfd_244 (Downloaded: 13/01/2025).
- Lévay, Gábor: *OSINT (Open Source Intelligence) – Nyílt információs hírszerzés.* Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2006.
- Márton, Balázs: *A nyílt forrású hírszerzés (OSINT) mint lehetőség a bűncselekmények felderítésében – A rendőrségen belüli önálló OSINT egység koncepciója*. Belügyi Szemle, Vol. 71, No. 8 (2023), 1419–1435. https://doi.org/10.38146/BSZ.2023.8.5
- Molnár, Tamás József: *Az internetes biztonság és az OSINT összefüggései*. Nemzetbiztonsági Szemle, Vol. 9, No. 2 (2021), 81–94. https://doi.org/10.32561/nsz.2021.2.6
- Nemzeti Információs Központ (National Information Center): *Nyílt forrású hírszerzés*. 2022. https://nik.gov.hu/nyilt-forrasu-hirszerzes (Downloaded: 13/01/2025).
- North Atlantic Treaty Organization: *NATO OSINT Handbook v1.2*. NATO, 2001. https://archive.org/details/nato-osint-handbook-v-1.2-jan-2002 (Downloaded: 13/01/2025).
- Orbán, Anna: *Információ*. Közszolgálati Online Lexikon, Nemzeti Közszolgálati Egyetem, [no year]. https://lexikon.uni-nke.hu/szocikk/informacio/ (Downloaded: 15/01/16.), Original source: 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 1. § Davenport, T. H. – Prusak, L.: Tudásmenedzsment, Kossuth Kiadó (Ford. Andor Éva), Budapest, 2001.
- Péter: *Hány videót töltenek fel naponta a YouTube-ra?* 2024. https://eoldal.hu/hany-videot-toltenek-fel-naponta-a-youtube-ra/ (Downloaded: 13/01/2025).
- *PUBLIC LAW 109–163.* National Defense Authorization Act for Fiscal Year 2006, Section 931, p. 3411. https://www.congress.gov/109/statute/STATUTE-119/STATUTE-119-Pg3136.pdf (Downloaded: 13/01/2025).
- Regényi, Kund Miklós: *OSINT a második generációs internetet megelőző korokban*. Nemzetbiztonsági Szemle, Vol. 7, No. 2 (2019), 32–37. https://doi.org/10.32561/nsz.2019.2.3
- Shaw, Sharline: *A legfontosabb YouTube-statisztikák és aktuális trendek 2025-ban*. (Key YouTube Statistics and Current Trends in 2025), LeeLine, 2025. https://www.ileeline.com/hu/youtube-statistics/#General_YouTube_Statistics (Downloaded: 13/01/2025).
- Solti, Imre: *Az OSINT információgyűjtő estközeiről*. Nemzetbiztonsági Szemle, Vol. 7, No. 2 (2019), 3–18. https://doi.org/10.32561/nsz.2019.2.1
- Szabadföldi, István: *A mesterséges intelligenciával támogatott nyílt információszerzés (OSINT) – evolúció és kihívások*. Nemzetbiztonsági Szemle, Vol. 10, No. 1 (2022), 30–51. DOI: 10.32561/nsz.2022.1.3
- Szabó, Károly: *Az OSINT – Gondolatok a tevékenységről, és az alkalmazás közegéről*. Nemzetbiztonsági Szemle, Vol. 7, No. 2 (2019), 68–82. https://doi.org/10.32561/nsz.2019.2.6

- Vakkari, Pertti – Cronin, Blaise (eds.): *Conceptions of Library and Information Science: Historical, Empirical and Theoretical Perspectives*. Taylor Graham, London, 1992.
- Vattai, Eszter: *A nyílt forrású információszerzés kapcsolata a hadsereggel*. Hadmérnök, Vol. 18, No. 2 (2023), 155–165. https://doi.org/10.32567/hm.2023.2.10
- Vida, Csaba: *Nyílt forrású adatszerzés (OSINT)*. In: Kobolka, István (ed.): Nemzetbiztonsági alapismeretek. Nemzeti Közszolgálati Egyetem, Budapest, 2013, 101–109.



Dániel Frankl

PATTERNS OF VIRTUAL REALITY USE AND ASSOCIATED SYMPTOMS: A COMPARATIVE STUDY OF CIVILIAN AND MILITARY USERS

DOI: 10.35926/HDR.2025.1.5

ABSTRACT: *Virtual Reality (VR) technologies have become integral to modern military training, offering substantial advancements in operational preparedness, decision-making, and mission effectiveness. NATO forces, including the United States, the United Kingdom, and increasingly Hungary, have embraced VR solutions to improve joint interoperability and enhance realism in training scenarios, resulting in notable gains in threat identification accuracy and overall personnel readiness. However, the successful deployment of VR in military contexts necessitates an in-depth understanding of physiological and neurological considerations, such as cybersickness, cognitive overload, visual fatigue, and ergonomic strain, each of which can significantly impact soldiers' cognitive performance and physical comfort. Empirical research conducted among military and civilian VR users reveals that military-trained individuals exhibit distinct psychological resilience, improved stress management, and heightened neurological adaptability compared to civilians. These measurable differences reinforce VR's value as a strategic training asset, particularly when supported by ergonomically optimized equipment and adaptive, neurophysiologically informed training protocols. Consequently, continued investment in human-centered VR development is essential to fully leverage the operational advantages offered by immersive training, enhancing both the efficacy and safety of military personnel in complex, real-world environments.*

KEYWORDS: *military training, immersive simulation, cognitive load, simulation technologies*

ABOUT THE AUTHOR:

Dániel Frankl is a PhD student at Óbuda University, Doctoral School on Safety and Security Sciences (ORCID: 0009-0002-5073-9412; MTMT: 10094319).

INTRODUCTION

The rapid advancement of Virtual Reality (VR) technologies in recent decades has profoundly transformed training methodologies across multiple sectors, particularly within defence and military operations.[1] Improvements in computational power, graphical rendering, and the availability of affordable yet sophisticated VR hardware have enabled military organizations to develop immersive, high-fidelity simulation environments. These advancements have attracted considerable attention from defence institutions worldwide, notably within NATO member states, due to VR's demonstrated potential to enhance operational realism, safety, and training efficiency.

[1] Leite – Vieira 2025.

Within the military domain, VR facilitates realistic simulations of complex and hazardous operational scenarios that would otherwise be impractical, resource-intensive, or unsafe to replicate in real-world conditions. However, alongside clear operational advantages, the integration of VR into military training introduces several physiological and neurological challenges. Issues such as cybersickness, cognitive overload, visual fatigue, ergonomic discomfort, and VR-induced stress pose significant barriers that must be thoroughly understood and effectively managed to ensure successful implementation. Recognizing both the opportunities and challenges associated with VR, NATO countries, including prominent adopters such as the United States and the United Kingdom, have actively integrated VR into their military training curricula, contributing valuable empirical insights and operational best practices. As a committed NATO member state, Hungary has similarly begun exploring VR's potential within its strategic modernization initiative, the Zrínyi 2026 Defence and Military Development Program,[2] explicitly highlighting immersive training technologies as instrumental tools for enhancing interoperability, readiness, and training effectiveness.

Given the strategic importance of VR technology for contemporary military preparedness, this paper systematically explores its applications, limitations, and physiological impacts within military contexts, emphasizing empirical comparisons between military and civilian users. It examines in detail how VR's physiological and neurological dimensions affect user experience and training outcomes, providing a scientific foundation for the continued adoption and refinement of immersive simulation technologies within defence frameworks. Ultimately, the publication aims to identify key factors critical to optimizing VR's utility and effectiveness, thereby directly contributing to enhanced military training standards, personnel resilience, and operational capability.

APPLICATION OF VR IN THE MILITARY AND THE DEFENCE SECTOR

Modern armed forces and defence organizations have begun integrating VR into a range of training and operational activities. This section surveys current implementations by NATO and several member states, notably the United States and the United Kingdom, as well as preliminary steps taken by the Hungarian Defence Forces.

As an alliance, NATO has recognized the value of virtual simulation for enhancing interoperability and readiness among its members. As early as 2003, a NATO technical report identified human–machine interface advances and cost-effectiveness as key reasons to pursue VR in military applications.[3] Since then, NATO countries have widely adopted VR across various military domains, often sharing technologies and lessons learned. In one recent NATO exercise (Toxic Trip 2023, a Chemical, Biological, Radiological and Nuclear defence drill), participants used an immersive VR platform to simulate hazardous environments and coordinate responses across allied units, demonstrating how virtual environments can allow distributed training where participants in different locations all "meet" in the same scenario.[4] NATO's Allied Command Transformation and the NATO Modelling and Simulation Centre of Excellence have been actively encouraging member states to develop interoperable VR training systems so that soldiers from different countries can train

[2] Kocsi – Kiss 2021.

[3] Lele 2013.

[4] Virtualware 2023.

together in shared virtual scenarios. These efforts align with NATO's broader strategic emphasis on digital innovation to enhance joint readiness.

The U.S. military has been a pioneer in adopting VR and related simulation technologies. One landmark program was the Dismounted Soldier Training System (DSTS), fielded in the early 2010s as the first immersive VR training system for infantry.[5] DSTS provided squads with networked VR stations where soldiers could move through virtual battlefields, employing their weapons with position trackers and experiencing 360° visual and auditory feedback. It allowed small units to practice urban operations, convoy security, room clearing, and other tactical scenarios without the need for extensive training grounds. An Army evaluation noted that DSTS could effectively support basic and advanced individual training, including mission rehearsal for urban combat, reconnaissance patrols, and convoy ambush drills, by enabling the repetition of scenarios that would be resource-intensive to set up physically.[6] Building on such experiences, the U.S. Army launched the Synthetic Training Environment (STE) initiative in the late 2010s. STE is an ambitious program aiming to unify live, virtual, and constructive (LVC) training under a common architecture by 2025. It envisions soldiers wearing VR/AR headsets to train in digitized replicas of real terrain, integrated with AI-driven entities, so that eventually, a brigade could conduct a coordinated exercise with some soldiers in simulators and others in the field, all seeing the same operational picture.[7] Early components of STE include the Integrated Virtual Trainers for dismounted troops, tank crews, and aviators, and a cloud-based platform to deliver training anywhere on demand. The U.S. has also used VR for specialized training, such as pilot and vehicle crew simulators (long standard in flight schools and armor units) and marksmanship trainers.[8] Moreover, American research has extended into using VR for resilience training, e.g., the Army Research Laboratory has tested VR combined with biofeedback to train soldiers in managing combat stress and fatigue.[9]

The UK's Ministry of Defence has similarly invested in VR to modernize training, particularly for the British Army and Royal Air Force. Under the Defence Innovation Fund (a £800 million program to spur new technologies), the UK has pursued the Virtual Reality in Land Training (VRLT) initiative.[10] This initiative seeks to evaluate how VR systems can augment or replace certain Army training activities to improve efficiency and reduce reliance on expensive real-world exercises. One notable collaboration is with Bohemia Interactive Simulations (BiSim), the developer of the Virtual Battlespace (VBS) series widely used in military simulators. The UK MoD contracted BiSim to develop a special VR module for its existing simulators, testing features such as high-resolution head-mounted displays integration, mixed reality for weapon handling, and enhanced after-action review tools. The integration of mixed reality enables soldiers to train with physical objects, such as replica rifles and mock control panels, while fully immersed in virtual scenarios. This approach has proven effective in developing muscle memory and familiarization with real-world equipment, as demonstrated by Ukrainian troops using US-supplied systems for

[5] Bymer 2012.

[6] Reitz – Richards 2013.

[7] Rozman 2020.

[8] Goldberg et al. 2023.

[9] Goodwin – Hoffman 2020.

[10] UK Government 2019.

combat preparation.[11] In addition to ground forces, the Royal Air Force has used VR for aircrew training and even recruitment outreach (e.g., VR flight demos at public events), and the Royal Navy is exploring VR for immersive mission planning and even submarine maintenance training.[12] As of 2025, the UK reached a milestone by certifying a mixed-reality Joint Terminal Air Controller (JTAC) training system (the CASE JTAC simulator using Varjo XR headsets) for official use, meaning NATO JTAC personnel can now maintain their qualifications through this VR-based system instead of some live exercises.[13] This is a clear testament to how far VR training has come, as a virtual/mixed reality system meets the rigorous standards for training elite personnel in calling in airstrikes, traditionally one of the most hands-on, live-training-intensive skills.

The use of VR in Hungary's military is still in the nascent stages, but recent initiatives and research efforts indicate a growing commitment. The Hungarian Defence Forces have historically relied on conventional training methods, but as the forces modernize, they recognize that simulation technologies must play a larger role in training and education. A clear sign of this shift is the establishment of the Innovation and Technology Directorate within the Ministry of Defence and the involvement of institutions like the National University of Public Service (NUPS) in studying military applications of VR.[14] Hungarian defence researchers have published analyses on how VR could enhance training effectiveness and what negative side effects to watch for. For example, Kovács conducted a series of studies on VR-based military training, examining factors that influence training efficacy and user acceptance among Hungarian soldiers.[15] The first part of his work outlined numerous potential applications of VR for the Hungarian defence sector – from virtual shooting ranges and tactical engagement simulators to VR-based maintenance training for complex equipment. The Hungarian Defence Forces have reportedly tested VR in a few specific contexts. One publicly demonstrated example is a VR system for parachute jump training, a 360-degree video simulator that allows paratrooper trainees to experience the visual sensation of a jump and practice emergency procedures (such as canopy malfunctions) in a virtual environment before any real airdrop. Another area of interest is engaging the younger generation of soldiers and cadets through digital means. In 2019, the HDF organized a "Digital Soldier 2.0" event in Budapest to showcase cutting-edge technologies; attendees could try out a VR tactical trainer that put them in a virtual combat scenario with a full-motion rig (allowing them to turn 360° and even feel motion cues).[16] This was not yet standard issue equipment, but it signaled intent by familiarizing cadets with VR. The HDF hope to build a culture of innovation where future forces will be comfortable with training in both real and virtual environments. Importantly, Hungary is also looking at how VR can support joint training with NATO allies. Through NATO's e-learning and training opportunities, Hungarian personnel have participated in VR-enhanced multinational exercises (for instance, Hungarian JTACs have used simulation systems similar to those of their British counterparts to practice coordination with Allied pilots).[17] While concrete programs (like a

[11] Epstein 2025.

[12] Royal Navy News 2023.

[13] Varjo 2025.

[14] Németh – Virágh 2021.

[15] Kovács 2024.

[16] Hegedűs – Sziválk 2019.

[17] Marlok – Takács 2024.

dedicated Hungarian VR training center) are still under development, the current trajectory suggests that the Hungarian Defence Forces would steadily increase their adoption of VR in the coming years, guided by both their pilot projects and the proven successes of larger allies.

PHYSIOLOGICAL AND NEUROLOGICAL FACTORS IN VIRTUAL REALITY

While VR holds significant potential for military training, its success depends on understanding and mitigating various physiological and neurological factors that influence user experience and performance. Military personnel require training environments not only to be realistic and immersive but also physiologically tolerable and neurologically manageable, ensuring optimal effectiveness and safety for training scenarios.

One primary physiological challenge associated with VR is cybersickness, often described as a form of simulator sickness.[18] Cybersickness manifests through a range of physiological symptoms such as nausea, dizziness, eye strain, and general disorientation.[19] Neurologically, it originates from sensory conflicts, discrepancies between visual cues perceived through VR and the vestibular signals received by the body. Such sensory mismatches provoke stress on neurological systems, particularly the vestibular and visual pathways, disrupting balance, orientation, and spatial awareness. Research shows that cybersickness is common, even in experienced users, impacting up to 60% of VR users to varying degrees.[20] These symptoms are particularly critical in military training, where physiological distress can severely impair cognitive and motor performance. For instance, if trainees experience dizziness or nausea, their cognitive capacity to process crucial training information diminishes, leading to compromised training outcomes or potential safety hazards. Military-specific research highlights cybersickness as a fundamental barrier that must be managed effectively. Methods of mitigation involve carefully structured exposure protocols, adaptive session durations, and possibly pharmacological interventions, such as motion sickness medication or natural supplements, to gradually build physiological tolerance among trainees.[21]

Alongside cybersickness, cognitive overload represents a critical neurological challenge in VR environments. The immersive nature of VR often involves intense sensory inputs, visual, auditory, and haptic cues that can exceed an individual's cognitive processing capacity. Cognitive load theory[22] asserts that excessive simultaneous demands on working memory can significantly degrade the efficiency of learning and task performance. Neurologically, the prefrontal cortex, responsible for executive functions and working memory, becomes particularly taxed when users encounter complex or multitasking scenarios, potentially leading to decreased task accuracy and decision-making impairments.[23]

[18] Vlahovic et al. 2024.

[19] Mousavi et al. 2013.

[20] Caserman et al. 2021.

[21] Dennison et al. 2016.

[22] Sweller et al. 2011.

[23] Miller – Cohen 2001.

In military VR training, scenarios are often inherently complex, simulating multifaceted operational environments that involve simultaneous demands such as navigation, communication, and threat assessment. If the neurological load exceeds manageable thresholds, trainees may struggle to process vital information, resulting in impaired performance and diminished training outcomes. Empirical research underscores the necessity of scenario and interface design that aligns cognitive demands with neurological capabilities, emphasizing intuitive interaction modalities to minimize unnecessary mental effort.[24] Innovative strategies include integrating authentic military equipment as controllers within VR environments, leveraging established neurological motor patterns and muscle memory to reduce cognitive load. Moreover, neurophysiological feedback mechanisms, such as heart rate variability and electroencephalography (EEG), offer valuable insights into trainees' real-time neurological states. The Australian Defence Force's "Performance Edge" initiative, for example, successfully utilized heart rate monitoring as biofeedback to adaptively tailor training difficulty, illustrating the potential for personalized, neurologically informed VR training environments.[25]

Physiological strain arising from prolonged VR use presents further challenges. Current VR hardware frequently causes physical discomfort through factors such as headset weight, uneven weight distribution, heat accumulation, and restricted fields of view.[26] Prolonged sessions may result in musculoskeletal strain, particularly neck and shoulder discomfort. Neurologically, continuous discomfort or pain sensations can distract trainees, diverting attention and cognitive resources away from critical training tasks. Thus, ergonomic considerations become essential in equipment design and session structuring, ensuring trainee comfort and optimal neurological engagement throughout VR experiences.

Eye strain represents another notable physiological concern with direct neurological implications. Extended exposure to VR environments increased demand on ocular muscles and visual neural pathways, potentially leading to blurred vision, dry eyes, or difficulty focusing.[27] These symptoms reflect neurological fatigue within visual perception pathways, which, if severe or prolonged, can degrade both short-term task performance and long-term visual health. Ensuring regular breaks and adjusting technical specifications, such as improved display refresh rates, resolution, and visual field ergonomics, can mitigate ocular fatigue and sustain neurological comfort during VR sessions.

Psychological and neurophysiological dimensions must also be considered, as certain VR scenarios may inadvertently induce stress, anxiety, or mild aggression. From a neurological standpoint, stress-related responses involve heightened activation of the autonomic nervous system, altering cardiovascular parameters and neural arousal states, which could either enhance or hinder performance depending on the context. Interestingly, research indicates that combat-experienced personnel exhibited significantly higher levels of perceived stress and were more prone to maladaptive coping mechanisms, including aggression.[28] These findings suggest that while military training provides foundational psychological preparation, prolonged or intense exposure to combat stressors can still result in elevated psychological strain rather than reduced sensitivity.

[24] Remigereau et al. 2024.

[25] Kluge et al. 2021.

[26] Ito et al. 2021.

[27] Hirzle et al. 2022.

[28] Lokyan et al. 2025.

Finally, issues related to cognitive disorientation and difficulty distinguishing between virtual and real-world contexts were reported infrequently among users in general.[29] This finding suggests that VR environments, despite their immersive realism, generally preserve robust neurological boundaries between virtual experiences and reality. However, even minimal disorientation risks warrant cautious consideration in critical military training scenarios to avoid potential neurological confusion in crucial operational moments.

In summary, the successful integration of VR into military training critically depends on a comprehensive understanding and careful management of physiological and neurological factors. Addressing cybersickness, cognitive overload, physical ergonomics, visual strain, and psychological responses through informed hardware design, tailored training protocols, and real-time neurophysiological feedback is paramount. As military organizations, including the Hungarian Defence Forces, continue to advance VR technologies and methodologies, prioritizing these human-centered considerations will be essential for optimizing the efficacy, safety, and acceptance of VR-based military training solutions.

RESEARCH METHODOLOGY

The primary aim of this research was to investigate patterns of Virtual Reality (VR) usage among different user groups and to assess potential physiological and neurological effects related to VR experiences. Specifically, the study addressed three core research questions: first, the frequency and purposes for which individuals utilize VR devices; second, the prevalence and nature of VR-related symptoms such as nausea, dizziness, or eye strain; and third, demographic or personal factors that might influence VR usage habits and the perception of associated side-effects. To address these questions, an online questionnaire-based survey was conducted in early 2025, employing convenience sampling. Recruitment took place primarily through various online platforms, including Discord communities, Telegram channels, Facebook interest groups, and university-wide email distributions. Initially, the survey yielded 290 responses, however, 85 respondents indicated no prior VR device usage. These responses were consequently excluded, resulting in 205 valid responses for subsequent analysis.

The questionnaire consisted of 14 targeted questions designed to investigate various dimensions of VR usage. Participants provided detailed information regarding their daily technology and gaming habits, VR device ownership, and frequency of VR use, rated on a 6-point scale (0 indicating "never" and 5 indicating "always"). Furthermore, respondents specified the predominant VR hardware type they employed, distinguishing between PC-connected and standalone headsets. Usage purposes were also recorded, covering entertainment, educational activities, creative tasks, social interaction, and fitness and health-related domains. Participants additionally reported the frequency and severity of experiencing side effects, such as cybersickness (nausea, dizziness), visual discomfort (eye strain, blurred vision), headaches, and psychological or physical symptoms, both during and after VR sessions. Finally, demographic characteristics, including age, gender, educational level, and professional background, were collected to enable subgroup comparisons.

The convenience sampling approach employed in this study naturally restricts the generalizability and representativeness of the findings to broader populations. Moreover, re-

[29] European Agency for Safety and Health at Work 2024.

liance on self-reported data inherently poses potential limitations related to recall inaccuracies and social desirability biases. Nevertheless, the study provides valuable initial insights into the comparative physiological and neurological impacts associated with VR usage. These findings offer a foundational basis for further controlled experimental studies exploring the complex interplay among user characteristics, VR engagement patterns, and the physiological and neurological implications of immersive virtual experiences.

RESULTS

Findings are presented in two sections: General Results (entire sample) and Military-Specific Results (participants with military affiliation). Prior to thematic analysis, respondent demographics are summarized to contextualize interpretation. The gender distribution of respondents revealed a clear male dominance, with 66% identifying as male and 34% as female.

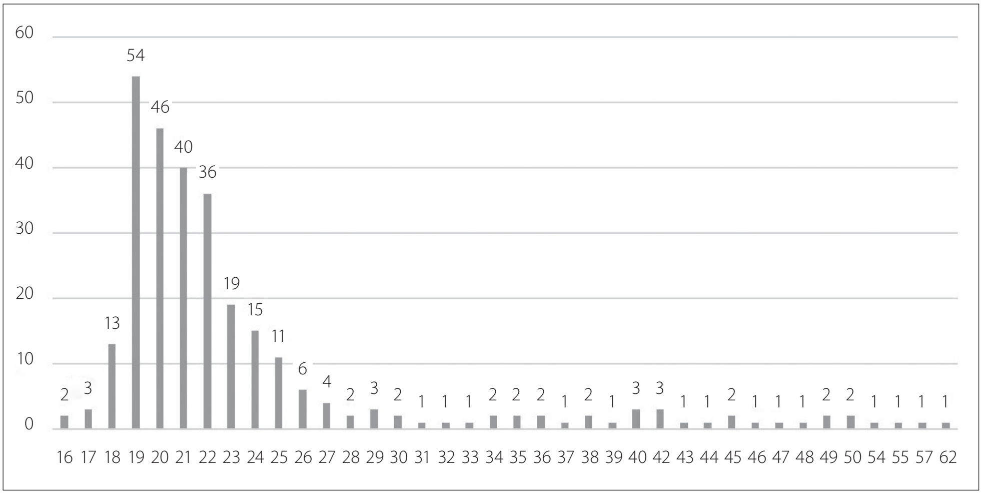


Figure 1 *Age distribution (Edited by the author based on research data)*

Figure 1 illustrates the age distribution. The mean age was 23.7 years (SD = 7.7), with a concentration in the 18–25 range and a peak at age 19. Since the questionnaire was distributed primarily through online tech and gaming communities, this age concentration was expected. However, it is important to note that the sample is not representative of the general population, which was considered when interpreting the results.

GENERAL RESULTS

Only 21% of respondents owned a VR device; however, 71% reported prior VR experience. Despite this exposure, usage frequency was low (mean = 2.00; SD = 1.10 on a 6-point scale). Device types included PC-tethered systems (37%), standalone units (25%), and unknown configurations (38%). Daily technology usage averaged 5.74 hours for work and 2.56 hours for gaming, indicating VR's presence beyond entertainment. Nonetheless, confidence in VR's professional integration remained low (mode = 2; mean = 2.84; SD = 1.41). Across application domains, entertainment showed the highest usage (mean = 2.92; SD = 1.73), while education, work, healthcare, creative use, social interaction, and sports scored substantially lower (means ≈ 1.4–1.6). Notably, domains such as healthcare and social VR, frequent in academic discourse, were rarely utilized in practice.

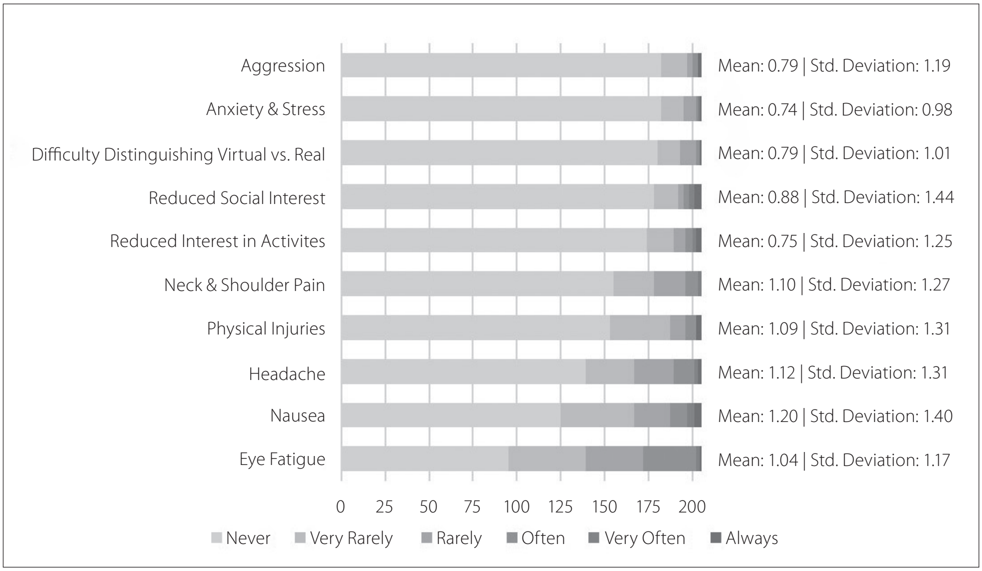


Figure 2 *Frequency of symptoms experienced during VR use*
(Edited by the author based on research data)

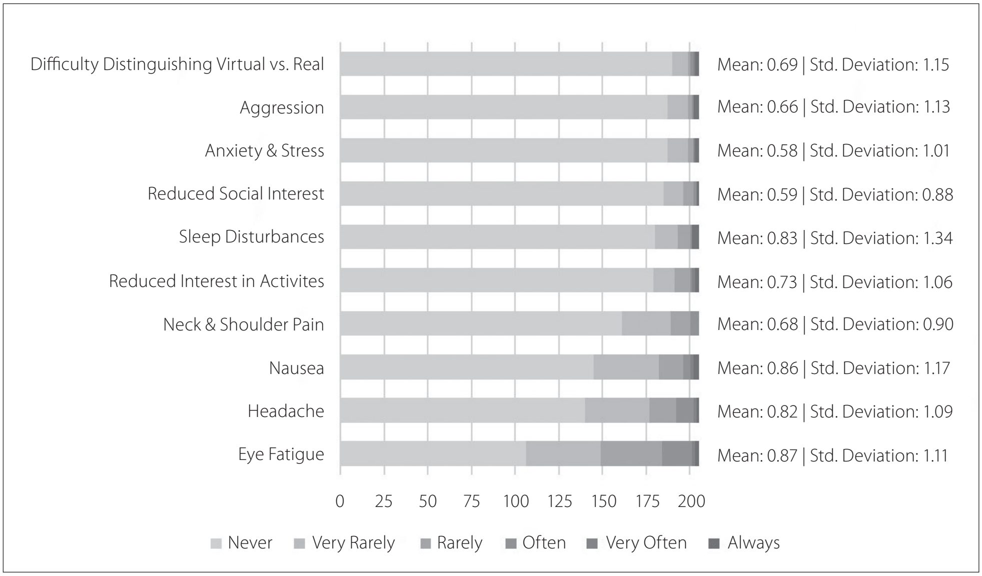


Figure 3 *Frequency of symptoms experienced after VR use*
(Edited by the author based on research data)

Figure 2 depicts in-use symptom prevalence. Nausea, headaches, and eye fatigue were most common (means ≈ 1.0), though typically infrequent. Physical discomfort (e.g., collisions, neck strain) was occasionally reported, consistent with VR's active nature. Psychological symptoms (e.g., disorientation, anxiety) were rare.

Figure 3 shows post-use effects, with eye fatigue, nausea, and headaches remaining the most reported symptoms (means $<$ 0.9). Mild sleep disturbances (mean = 0.83) were more prevalent than expected, potentially linked to cognitive overstimulation. Post-session psychological impacts remained minimal.

Overall, results indicate that while VR is primarily used for entertainment and is generally well-tolerated, mild physical discomfort and residual fatigue are common. These findings align with prior studies on cybersickness and immersive ergonomics.

MILITARY-SPECIFIC RESULTS

The military-affiliated subgroup (n = 73) comprised respondents with military service or military-related education. Comparative analysis was conducted using independent samples t-tests to examine differences in VR usage, application domains, and symptomatology between military and civilian participants. Both groups were predominantly aged 19–22, reflecting typical early-career and educational stages. Military respondents exhibited a broader variance in daily digital work activity, with usage peaks at 4 hours (20.5%) and 6 hours (17.8%), and isolated reports of prolonged use (14–24 hours), likely reflecting duty-related digital operations. In contrast, civilians showed a more centralized distribution around standard full-time work durations (2–8 hours). A notable 6.8% of the military group reported zero daily digital use, suggesting either analog roles or periods of digital abstinence due to operational protocols.

Gaming activity differed significantly: 24.7% of the military group reported no daily gameplay versus significantly lower rates among civilians. This discrepancy may reflect stricter discipline, limited leisure time, or institutional culture discouraging gaming. Conversely, isolated outliers in the military group reported extended gaming sessions, possibly indicating stress-coping behaviors or off-duty recreation. VR device ownership was low in both groups but more limited among military participants (16.4% vs. 22.1%). Nonetheless, prior VR exposure was comparable (~70%), indicating widespread familiarity independent of ownership. Military respondents showed slightly higher optimism towards VR's future utility in professional contexts, potentially reflecting exposure to simulation training environments. However, mean confidence levels remained moderate across both groups, indicating cautious outlooks. VR engagement remained infrequent overall. Both groups primarily used VR for entertainment purposes (gaming, immersive media), while professional, educational, and health-related applications were minimal. Military respondents showed marginally lower usage of PC-tethered VR systems, likely due to access limitations or operational impracticality.

Statistically significant differences emerged in psychological responses. Military-trained participants reported substantially lower anxiety and stress during VR use ($t = 4.316$, $p < .001$), less difficulty distinguishing virtual from real environments ($t = 3.431$, $p = .001$), and fewer sleep disturbances ($t = 3.840$, $p < .001$). Mean scores in these categories approached zero, indicating minimal symptomatology, while civilian responses displayed greater variability and higher averages. These results suggest enhanced psychological resilience in the military subgroup, likely attributable to stress inoculation training, exposure to simulated combat scenarios, and structured cognitive conditioning inherent to military instruction. Physiological symptoms, eye strain, headaches, and physical discomfort showed no significant differences between groups. High intra-group variance limited statistical power in these domains, suggesting that physical responses to immersive technology are more universally distributed, regardless of background. The military group was overwhelmingly male (t=11.844, p<.001) and significantly less likely to possess IT-related qualifications (t=6.919, p<.001), reflecting divergent professional pipelines. The binary group variable (military vs. non-military) yielded a highly significant differentiation (t=-26.129, p<.001), confirming structural separation and validating comparative subgroup analysis.

Overall, military-trained individuals demonstrate higher psychological tolerance and stability during VR exposure, likely linked to their unique training and operational environment. However, physical effects appear consistent across user groups. These findings underscore the moderating role of military experience in immersive technology contexts and suggest operational advantages in training resilience through VR platforms.

CONCLUSION

Virtual Reality (VR) represents a strategic asset in modern military training, enhancing decision-making, threat recognition, and mission readiness. NATO forces, particularly the US and the UK, have demonstrated effective implementation through programs such as the US Army's Synthetic Training Environment (STE) and the UK's Virtual Reality in Land Training (VRLT), showcasing VR's capacity for realistic, cost-efficient, and interoperable training. While still in early adoption phases, the Hungarian Defence Forces also signal intent to integrate immersive systems to strengthen operational effectiveness within NATO frameworks.

VR efficacy is closely tied to physiological and neurological factors, including cybersickness, cognitive overload, ergonomic strain, and stress reactivity. Without proper design, prolonged exposure may impair performance. However, adaptive training protocols incorporating ergonomic design and neurophysiological feedback (e.g., biofeedback-driven scenario adjustments) have proven effective in mitigating these issues, improving cognitive load management, and operational resilience.

Empirical data confirm that compared to civilian users, military-trained users exhibit higher psychological stability, reduced anxiety, and enhanced neurocognitive differentiation between virtual and real environments. While physical symptoms such as eye strain and headaches remain common, the psychological advantages among military personnel highlight the impact of structured, stress-adaptive VR exposure on combat readiness.

Overall, VR offers significant strategic value by optimizing training efficiency, reinforcing cognitive resilience, and minimizing logistical demands. Future development should prioritize human-centered design, integrating physiological, neurological, and ergonomic considerations to fully realize VR's potential in complex defence scenarios and sustain military readiness.

BIBLIOGRAPHY

- Bymer, Loren, Maj.: *DSTS: First immersive virtual training system fielded*. U.S. Army, 1 August 2012. https://www.army.mil/article/84728/dsts_first_immersive_virtual_training_system_fielded (Accessed: 5/4/2025).

- Caserman, Polona – Garcia-Agundez, Augusto – Zerban, Alvar Gámez – Göbel, Stefan: *Cybersickness in current-generation virtual reality head-mounted displays: systematic review and outlook*. Virtual Reality, Vol. 25, 2021, 1153–1170. DOI: 10.1007/s10055-021-00513-6
- Dennison, Mark S. – Wisti, A. Zachary – D'Zmura, Michael: *Use of physiological signals to predict cybersickness*. Displays, Vol. 44, 2016, 42–52. DOI: 10.1016/j.displa.2016.07.002
- European Agency for Safety and Health at Work: *Worker Exposure to Virtual and Augmented Reality and Metaverse Technologies: How Much Do We Know?* Discussion paper, 2024. https://osha.europa.eu/sites/default/files/documents/worker-exposure-virtual-reality_discussion_paper_EN.pdf (Accessed: 5/4/2025).
- Epstein, Jake: *Inside the virtual battles Ukrainian soldiers are fighting with top-of-the-line fake guns to train for real combat*. Business Insider, 15 March 2025. https://www.businessinsider.com/how-ukrainian-troops-fight-fake-guns-prepare-for-real-combat-2025-3 (Accessed: 5/4/2025).
- Goldberg, Benjamin – Spain, Randall – Owens, Kevin – Lanman, Jeremy – Kwon, Paul, Col. – Gupton, Kevin – McGroarty, Chris – Butler, Paul: *A Data Strategy for Data-Driven Training Management: Artificial Intelligence and the Army's Synthetic Training Environment*. Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC), 2023.
- Goodwin, Gregory A. – Hoffman, Michael: *Intelligent adaptive training in the synthetic training environment, 2020 update*. In: Sinatra, Anne M. (ed.): Proceedings of the 8th Annual Generalized Intelligent Framework for Tutoring (GIFT) Users Symposium (GIFTSym8). US Army Combat Capabilities Development Command–Soldier Center, 2020, 113–119. ISBN 978-0-9977258-0-3.
- Hegedűs, Ernő – Szivák, Petra: *A jövő digitális katonája és kognitív képességei − beszámoló a Digital Soldier 2.0 nemzetközi konferenciáról*. Haditechnika, Vol. 53, No. 3 (2019), 52–57. DOI: 10.23713/HT.53.3.10
- Hirzle, Teresa – Fischbach, Fabian – Karlbauer, Julian – Jansen, Pascal – Gugenheimer, Jan – Rukzio, Enrico – Bulling, Andreas: *Understanding, Addressing, and Analysing Digital Eye Strain in Virtual Reality Head-Mounted Displays*. ACM Transactions on Computer-Human Interaction. Vol. 29, No. 4 (2022), 1–80. DOI: 10.1145/3492802.
- Kluge, Murielle G. – Maltby, Steven – Walker, Nicole – Bennett, Neanne – Aidman, Eugene Nalivaiko – Walker, Frederick Rohan: *Development of a modular stress management platform (Performance Edge VR) and a pilot efficacy trial of a bio-feedback enhanced training module for controlled breathing*. PLOS One, Vol. 16, No. 2 (2021). DOI: 10.1371/journal.pone.0245068.
- Kocsi, János Gyula – Kiss, Gergely László: *Challenges of the Application of Lynx KF-41 Infantry Fighting Vehicle in the Hungarian Defence Forces*. Hadmérnök, Vol. 16, No. 4 (2021), 25–40. DOI: 10.32567/hm.2021.4.3
- Kovács, Gergely: *A védelmi szférában alkalmazható VR-alapú képzés/felkészítés lehetséges negatív fizikai és pszichológiai hatásai II.* (Possible Negative Physical and Psychological Effects of VR-Based Training/Preparation in the Defence Sector II.) Hadmérnök, Vol. 18, No. 4 (2024), 31–51. DOI: 10.32567/hm.2023.4.3.
- Ito, Kodai – Tada, Mitsunori – Ujike, Hiroyasu – Hyodo, Keiichiro: *Effects of the Weight and Balance of Head-Mounted Displays on Physical Load*. Applied Sciences, Vol. 11, No. 15 (2021), 6802. DOI: 10.3390/app11156802
- Leite, Higor – Vieira, Leandro R.: *The use of virtual reality in human training: trends and a research agenda*. Virtual Reality, Vol. 29, No. 25 (2025). DOI: 10.1007/s10055-024-01093-x.
- Lele, Ajey: *Virtual reality and its military utility.* Journal of Ambient Intelligence and Humanized Computing, Vol. 4, 2013, 17–26. DOI: 10.1007/s12652-011-0052-4.
- Lokyan, Arsen – Baghdasaryan, Svetlana – Hovhannisyan, Hayk: *Enhancing psychological training in military personnel: Modern approaches, systemic assessments and hands-on*

recommendations. Asian Journal of Psychiatry, Vol. 106 (104442), 2025. DOI: 10.1016/j.ajp.2025.104442

- Marlok, Tamás – Takács, Márk György: VR *Training Opportunities in the Hungarian Defence Forces*. Academic and Applied Research in Military and Public Management Science (AARMS), Vol. 23, No. 2 (2024), 19–37. DOI: 10.32565/aarms.2024.2.2.
- Miller, Earl K. – Cohen, Jonathan D.: *An integrative theory of prefrontal cortex function*. Annual Review of Neuroscience, Vol. 24, No. 1 (2001), 167–202. DOI: 10.1146/annurev.neuro.24.1.167.
- Mousavi, Maryam – Jen, Yap Hwa – Musa, Siti Nurmaya Binti: *A Review on Cybersickness and Usability in Virtual Environments*. Advanced Engineering Forum, Vol. 10, 2013, 34–39. DOI: 10.4028/www.scientific.net/aef.10.34.
- Németh, András – Virágh, Krisztián: *Virtuális valóság és haderő – katonai alkalmazási lehetőségek IV. rész*. Haditechnika, Vol. 55, 2021, 2–7. DOI: 10.23713/HT.55.5.01.
- Reitz, Emilie – Richards, Robert: *Optimum Dismounted Soldier Training Experience: Live or Virtual?* I/ITSEC 2013.
- Remigereau, Alexis – Darses, Françoise – Dozias, Baptiste – Albentosa, Julie: *Design and validation of a simulated multitasking environment for assessing the cognitive load on the infantry squad leader*. Frontiers in Psychology, Vol. 15, 2024, DOI: 10.3389/fpsyg.2024.1433822
- Royal Navy News: *Royal Navy Enters the Metaverse with New Virtual Reality Simulators*. 14 February 2023. https://www.royalnavy.mod.uk/news/2023/february/14/20231402-vr-bridge-sims (Accessed: 5/4/2025).
- Rozman, Jeremiah: *The Synthetic Training Environment*. Association of the United States Army, Spotlight 20-6, 2020.
- Sweller, John – Ayres, Paul – Kalyuga, Slava: *Cognitive Load Theory*. Springer, 2011. DOI: 10.1007/978-1-4419-8126-4
- UK Government: *British Army tests innovative virtual reality training*. 4 February 2019. https://www.gov.uk/government/news/british-army-tests-innovative-virtual-reality-training (Accessed: 5/4/2025).
- Varjo: *Varjo XR-4 Achieves NATO Accreditation in Inzpire's Cutting-Edge JTAC Simulator*. 17 January 2025. https://varjo.com/press-release/varjo-xr-4-achieves-nato-accreditation-in-inzpires-cutting-edge-jtac-simulator/ (Accessed: 5/4/2025).
- Virtualware: *Virtualware's VIROO capabilities shown at NATO Exercise*. 29 September 2023. https://www.virtualwareco.com/news/viroo-showcased-at-nato-exercise-toxic-trip-2023/ (Accessed: 5/4/2025).
- Vlahovic, Sara – Skorin-Kapov, Lea – Suznjevic, Mirko – Pavlin-Bernardic, Nina: *Not just cybersickness: Short-term effects of popular VR game mechanics on physical discomfort and reaction time*. Virtual Reality, Vol. 28, 108, 2024. DOI: 10.1007/s10055-024-01007-x.

Péter Szikora

WHO CAN SUPPORT THE INTRODUCTION OF SELF-DRIVING MILITARY VEHICLES?

DOI: 10.35926/HDR.2025.1.6

ABSTRACT: *The aim of the current paper is to map attitudes towards self-driving vehicles along eight key questions, which look at the challenges of the technology, risk perception, and potential civil and military uses. The results show that trust in the cybersecurity of self-driving cars is strongly correlated with fear of new technologies, privacy concerns, and fear of failure. Respondents with confidence towards self-driving technology are more open to military applications, while those without confidence have higher concerns about controllability. The cluster analysis identified three distinct clusters of attitudes: negative perceptions, cautiously open, and technology-friendly. The results highlight the diversity of trust patterns and contribute to a better understanding of the social acceptance of autonomous vehicles.*

KEYWORDS: *autonomous vehicles, cybersecurity, military applications, regulation, terrorism risks*

ABOUT THE AUTHOR:

Péter Szikora is an associate professor at Óbuda University, Keleti Károly Faculty of Business and Management (ORCID: 0000-0001-8680-3880; MTMT: 10020399).

SELF-DRIVING CARS

Self-driving cars represent one of the most divisive areas of technological development, as they raise a number of social, legal, and ethical issues. The operation of self-driving cars is based on different levels of automation. SAE International[1] distinguishes six levels, ranging from full manual control to full autonomy. However, the introduction of such systems faces a number of legal and ethical hurdles, particularly in the European Union, where the Vienna Convention requires all vehicles to have a human driver (United Nations, 1968).[2] In contrast, the uptake of self-driving cars in the United States is proceeding at a faster pace, with the National Highway Traffic Safety Administration (NHTSA) setting strict safety standards for these vehicles.[3] In China, the development of self-driving technology is also proceeding at a rapid pace, encouraged by extensive government support for research and development.[4]

One of the biggest challenges for autonomous vehicles is gaining public trust. Studies have shown that people's attitudes are significantly influenced by age, gender, education, and attitude towards technology.[5] While the economic interests of manufacturers make it crucial to achieve widespread uptake of the technology as soon as possible, an interpretative approach can help to gain a deeper understanding of people's reactions and concerns.[6]

[1] Brooke 2016.

[2] United Nations 1968; see more: https://net.jogtar.hu/jogszabaly?docid=98000005.tvr.

[3] Atiyeh 2021.

[4] Li et al. 2022.

[5] Jaradat et al. 2020; König – Neumayr 2017.

[6] Gál et al. 2024.

Industry players try several strategies to increase user confidence, such as demonstration programmes and educational campaigns for the public.[7] Surveys have shown that the majority of people are sceptical about the introduction of self-driving cars, mainly because of their price and reliability. A 2014 study found that people in the US, UK, and Australia did not feel prepared to use fully autonomous vehicles. In contrast, research by Kyriakidis and colleagues showed that people are more open to self-driving cars, especially when those are introduced in public transport.[8] Research by Kettles and Van Belle, on the other hand, found that the majority of people would not use these vehicles for at least six months after their introduction.[9] Another study found that 67% of people feared software failures in self-driving vehicles.[10] Other research has shown that people are more likely to adopt autonomous transport devices if they are used in situations where they could reduce the number of accidents, such as in severe weather conditions or during long-distance driving.[11]

One of the key ethical challenges for self-driving cars is the need for vehicles to be able to make decisions in accident situations. People generally accept the principle that the vehicle should make decisions with the least possible sacrifice, but when it comes to their own lives, they take a different view.[12] For this reason, the continuous development of self-driving car software and addressing ethical dilemmas are essential to increase the reliability of the technology.[13] According to some philosophical schools of thought, the application of such technologies can only be ethical if they follow the principles of human decision-making.[14] Part of the debate on the ethics of self-driving cars centres on the extent to which the manufacturer, the programmer, or even the user of the car can be held liable in the event of an accident.[15] In conclusion, the development of self-driving car technology poses not only technological but also social and ethical challenges. Gaining public trust, legal regulation issues, and ethical decision-making are all factors that will have a significant impact on the future uptake of autonomous vehicles. As the technology develops, it will become increasingly inevitable that society finds a clear answer on how to integrate these vehicles safely and ethically into everyday transport.

SELF-DRIVING CARS AND TERRORISM

The development of autonomous systems in the automotive and military sectors raises new questions of responsibility and security. Bo draws attention to the fact that the role of programmers in the development of autonomous systems is not limited to their creation, but also extends to the ongoing monitoring of their operation.[16] According to the principle of Meaningful Human Control (MHC), programmers may be liable for crimes committed by autonomous systems if they could have foreseen the risks and failed to take appropriate steps to minimise them.

[7] Schoettle 2016.
[8] Kyriakidis et al. 2015.
[9] Kettles – Van Belle 2019.
[10] Howard – Dai 2014.
[11] Cavoli et al. 2017.
[12] Servin et al. 2023; Goodall 2014.
[13] Woollard 2023.
[14] Borenstein et al. 2019.
[15] Gogoll – Müller 2017.
[16] Bo 2022.

The link between cybersecurity and terrorism is also of growing importance. According to Perger, cyberterrorism includes cyberattacks that may be aimed at crippling infrastructure or achieving political goals.[17] The use of military drones raises new issues in international law, while cyber defence and information security play a key role in threat reduction. Kumar concludes that terrorist organisations can use technology to coordinate their attacks more effectively, and therefore, defence strategies must include both human and technological elements.[18]

Several studies in the field of autonomous vehicles have highlighted security and societal challenges. According to Viktor and Fodor, self-driving technology is not developing as fast as many expected, mainly due to gaps in V2V communication and data security.[19] The research highlights that self-driving cars are less of a threat from a terrorism perspective, but the potential for group attacks makes the development of secure communications essential. Human factors also play a key role in the operation of autonomous systems. According to Kovács, Hőgye-Nagy, and Kurucz, situational awareness is essential for the success of interactions between autonomous vehicles and humans.[20] Psychological research suggests that increasing user awareness can improve the safe use of autonomous vehicles. Chougule and colleagues investigated the causes of accidents involving self-driving cars and found that weather conditions, cybersecurity threats, and infrastructure deficiencies are significant barriers to the development of the technology.[21] Ethical and legal regulations require further research to ensure that autonomous systems can be safely integrated into transport.

Social acceptance is also an important factor for the uptake of autonomous vehicles. Research by Othman has shown that accidents involving self-driving cars have a negative impact on public opinion, especially in Europe.[22] However, demographics show a greater interest in autonomous vehicles in developing countries. Szatmáry and Lazányi sought to answer the question of whether self-driving cars are actually safer than conventional vehicles.[23] Their research suggests that the advanced sensing and response capabilities of autonomous vehicles can help reduce accidents, but that infrastructure, regulation, and public confidence remain challenges to the widespread uptake of the technology. Further investigation into the development of autonomous systems is needed to ensure that the issue of liability is clearly defined for both developers and users.

The use of artificial intelligence and machine learning brings the capabilities of autonomous systems to new levels, but also increases the potential risks. The ethical dilemmas arising from the operation of autonomous vehicles and weapon systems generate serious legal and societal debates. Technological advances have a significant impact not only in transport and warfare, but also in healthcare and industrial automation. Artificial intelligence-led diagnostic systems play an increasing role in medicine, while in industry, autonomous robots can increase productivity and reduce the risks of human labour. Social

[17] Perger 2022.

[18] Kumar 2019.

[19] Viktor – Fodor 2024.

[20] Kovács et al. 2021.

[21] Chougule et al. 2023.

[22] Othman 2023.

[23] Szatmáry – Lazányi 2022.

acceptance and regulation will remain key factors in the development of autonomous systems, and future research will aim to integrate these technologies into everyday life in a safe and ethical way.

RESEARCH METHOD

The research methodology relies exclusively on primary data and thus provides a comprehensive picture of the acceptance of self-driving cars directly through the opinions and experiences of the respondents. The research was conducted using convenience sampling, adapted to the resources available. Examining age, gender, education, and technological affinity helps to reveal the correlations behind individual attitudes. Descriptive statistical methods, Spearman correlation, and independent samples t-test were used to present the research findings using SPSS 25 software. Although the research is not representative of the whole population, the results point to important correlations. Statistical conclusions should take into account the limitations of the sample, as generalisability is not guaranteed. There are several reasons to investigate the adoption of self-driving cars: firstly, the influence of the regulatory environment and secondly, to understand individual attitudes towards the use of the technology.

SAMPLE PRESENTATION

The data for the survey was collected using an anonymous online questionnaire, which proved to be an ideal tool to ask for opinions on sensitive or divisive topics. Ensuring anonymity helped respondents to share their opinions honestly, as they did not need to fear being identified, which is particularly important in issues such as the public perception of self-driving cars, where views may differ. An additional advantage of the online format was that it allowed for a quick and efficient collection of responses and the immediate digitisation of the data obtained, which also greatly facilitated and accelerated the analysis process.

The self-completion format used in the online survey allowed respondents to complete the questionnaire at their own pace, in a comfortable environment, at any time, which could not only increase the willingness to respond but also contribute to the thoughtfulness of the responses. While this type of data collection does present some methodological challenges, such as response rates or representativeness, the aim of the survey was not to provide a representative sample of the population as a whole, but to gain insight into the social acceptance of self-driving vehicles through a broad sample, reflecting a wide range of opinions. This objective was well served by the methodology used.

The sample of respondents after the cleaning steps, before data processing, was 277. This was a sufficient number of respondents to draw reliable statistical conclusions. The age distribution of the sample is illustrated in Figure 1. The age of the respondents ranged from 10 to 78 years, which gives a wide age coverage. The mean age was 27.79 years and the median age was 21 years, indicating that the sample was predominantly over-represented in younger age groups. This may be particularly useful as the views of the younger generations may be of particular importance for the future social acceptance of a technology.

The research explored attitudes towards self-driving technologies along eight targeted questions, covering perceived challenges, risks, and potential uses of autonomous vehicles. The dimensions surveyed provide a comprehensive picture of respondents' views on

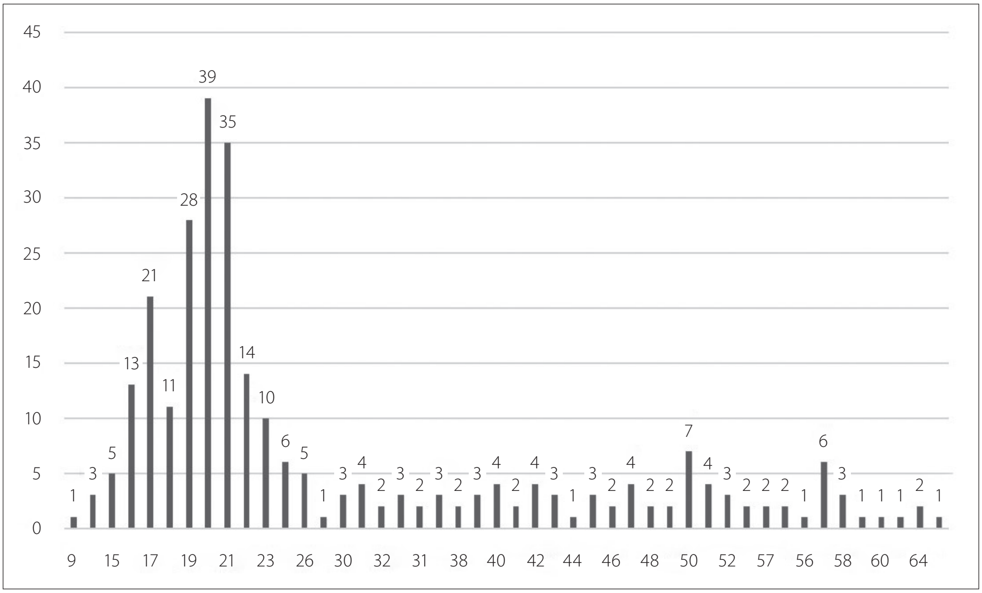


Figure 1 *Age distribution of respondents (n = 277)*

both civilian and military applications. The following variables formed the basis of the analysis:

- Biggest technological challenge: The question aims to find out what respondents consider to be the biggest technological challenge in the development and deployment of self-driving vehicles. The responses will help identify the main barriers limiting technological adoption.
- Cybersecurity of self-driving cars: This question explores concerns about the cybersecurity risks of self-driving vehicles. The answers provide an indication of the extent to which respondents feel vulnerable to hacking and unauthorised access.
- Communication between drivers and pedestrians: This question measures the importance respondents attach to the establishment of effective communication between self-driving vehicles and human road users. This issue is particularly relevant in the context of urban transport, where implicit human interaction is common.
- Need for regulation: This question addresses the need for a regulatory framework for autonomous vehicles. Respondents express their views on the importance of regulating responsibility, ethics, and safety at the level of legislation.
- Most challenging traffic environment: This question asks respondents which traffic environment (e.g., city, motorway, extreme weather) they consider most challenging for self-driving systems. The results highlight socially perceived technological barriers.
- Combat use of self-driving military vehicles: This question explores societal attitudes towards the use of autonomous vehicles for combat purposes in the military. It focuses on the acceptability of military decision-making without human intervention.
- Most suitable military tasks for self-driving vehicles: This question explores which military tasks (e.g., logistics, reconnaissance, surveillance, combat) respondents consider most suitable for autonomous vehicles. The results contribute to the societal perception of autonomous military technology developments.

- Likelihood of terrorist use: This question assesses the extent to which respondents fear that self-driving vehicles could be used for malicious purposes, such as terrorist attacks. The answers reflect societal perceptions of the technological threat.

RESULTS

Table 1 *Correlation table*

		Biggest technological challenge	Cybersecurity of self-driving cars	Communication between drivers and pedestrians	Need for legal regulation of self-driving cars	Most challenging transport environment	Combat applications of self-driving military vehicles	The most suitable military tasks for self-driving vehicles	Likelihood of terrorist use of self-driving vehicles
Hackers hack into car systems	**Correlation Coefficient**	.084	-.316**	.200**	.204**	-.050	-.066	.006	.188**
	Sig. (2-tailed)	.164	.000	.001	.001	.410	.273	.924	.002
The self-driving car breaks down	**Correlation Coefficient**	.070	-.320**	.293**	.353**	-.207**	-.128*	-.044	.221**
	Sig. (2-tailed)	.245	.000	.000	.000	.001	.034	.470	.000
Fear of new technology	**Correlation Coefficient**	.151*	-.288**	.120*	.066	-.046	-.171**	-.091	.103
	Sig. (2-tailed)	.012	.000	.045	.270	.444	.004	.131	.088
People lose their jobs because of it (e.g., taxi drivers)	**Correlation Coefficient**	.101	-.278**	.139*	.124*	-.143*	-.118*	-.085	.059
	Sig. (2-tailed)	.092	.000	.020	.039	.017	.049	.160	.326
Control cannot be taken back	**Correlation Coefficient**	.020	-.341**	.231**	.232**	-.059	-.139*	-.041	.126*
	Sig. (2-tailed)	.736	.000	.000	.000	.326	.020	.501	.037
Too expensive	**Correlation Coefficient**	.033	-.116	.135*	.105	-.127*	-.032	.001	.108
	Sig. (2-tailed)	.582	.055	.024	.082	.034	.593	.983	.072
The driving experience is lost	**Correlation Coefficient**	.057	-.153*	.168**	.283**	-.102	.049	-.104	.052
	Sig. (2-tailed)	.348	.011	.005	.000	.089	.421	.084	.393
Lack of security of personal data	**Correlation Coefficient**	.131*	-.367**	.143*	.244**	-.093	-.053	-.084	.131*
	Sig. (2-tailed)	.030	.000	.017	.000	.124	.383	.162	.030

		Biggest technological challenge	Cybersecurity of self-driving cars	Communication between drivers and pedestrians	Need for legal regulation of self-driving cars	Most challenging transport environment	Combat applications of self-driving military vehicles	The most suitable military tasks for self-driving vehicles	Likelihood of terrorist use of self-driving vehicles
Gender	**Correlation Coefficient**	.042	-.209**	.127*	.125*	-.078	-.146*	-.119*	.129*
	Sig. (2-tailed)	.482	.000	.035	.037	.198	.015	.048	.032
Age	**Correlation Coefficient**	.148**.*	-.212**	.230**	.228**	-.107	.099*	.004*	.294**
	Sig. (2-tailed)	.014	.000	.000	.000	.076	.099	.941	.000
Residence	**Correlation Coefficient**	-.013	.121*	-.049	-.011	.020	-.040	-.026	-.088
	Sig. (2-tailed)	.830	.044	.417	.858	.742	.507	.663	.143
Education	**Correlation Coefficient**	.160**	-.228**	.113	.196**	-.090	.027	.059	.254**
	Sig. (2-tailed)	.007	.000	.060	.001	.135	.656	.327	.000
Studies	**Correlation Coefficient**	-.117	.094	-.055	-.045	.065	-.018	.095	-.052
	Sig. (2-tailed)	.053	.118	.360	.458	.280	.765	.116	.392

There is a medium-strong negative relationship between trust in the cybersecurity of self-driving cars and fear of hacker attacks (correlation coefficient: -0.316; p: 0.000). This means that the more one fears hacker attacks, the less one trusts the cybersecurity of self-driving cars. There is a medium-strong positive relationship between the need for legal regulation of self-driving cars and fear of self-driving car failures (correlation coefficient: 0.353; p: 0.000). This suggests that those who are more concerned about technological failures see a greater need for the development of a legal framework. There is a negative relationship of medium strength (correlation coefficient: -0.288; p: 0.000) between trust in the cybersecurity of self-driving cars and fear of technological innovations. This suggests that those who fear new technologies are less confident in the security of self-driving cars. There is a weak negative relationship between confidence in the cybersecurity of self-driving cars and fear of job losses (correlation coefficient: -0.278; p: 0.000), suggesting that those who fear that self-driving technology will eliminate jobs are less confident in the safety of self-driving cars. There is a weak positive relationship between the need for legal regulation of self-driving cars and the fear of not being able to take control back (correlation coefficient: 0.232; p: 0.000), suggesting that those who fear that they would not be able to take control back in an emergency would give more importance to improving legal regulation. There is a negative relationship of medium strength (correlation coefficient: -0.367; p: 0.000) between trust in the cybersecurity of self-driving cars and lack of security of personal data, indicating that those who are concerned about the protection of personal data are less trusting of the cybersecurity of self-driving cars. However, there is a weak positive relationship between the lack of personal data security and the need for legal regulation of self-driving cars (correlation coefficient: 0.244; p: 0.000), indicating that those with greater privacy concerns consider it more important to strengthen legal regulation. There is a weak positive relationship between the need to improve communication between self-drivers and pedestrians and age (correlation coefficient: 0.230; p: 0.000), indicating that older people feel a greater need for this type of improvement. Similarly, there is a weak positive relationship between age and the need for legal regulation of self-driving cars (correlation coefficient: 0.228; p: 0.000), suggesting that older people consider it more important to clarify liability issues. Finally, there is a weak positive relationship between the highest educational attainment and the need for legal regulation of self-driving cars (correlation coefficient: 0.196; p: 0.001). This indicates that more highly educated people perceive a greater need for clarification of legal regulation.

In analysing the data, a t-test was used to see whether there is a significant difference between those who trust self-driving technology and those who do not. The results show a significant difference in several cases, supporting the previous correlation analysis. The t-test shows a significant difference between those who distrust and those who trust in several aspects, such as fear of new technology. Those who trust less in self-driving technology have a higher fear of the risks of new technologies (mean = 3.22) than those who trust (M = 2.32). The difference is significant (t = 2.502; p = 0.019). The possibility of taking control back: the distrustful (mean = 4.12) are more concerned about not being able to take control back in case of an emergency than the trustful (M = 3.09). The t-test result indicates a significant difference (t = 3.977; $p < 0.001$). Combat deployment of self-driving military vehicles: those less confident in the technology (M = 2.57) are less likely to consider the combat deployment of such vehicles acceptable than those who are confident (M = 3.05). The difference is significant (t = -2.166; p = 0.032). Likelihood of terrorist use: those who lack confidence (M = 2.92) are less likely than those who have confidence (M = 3.36) to believe that terrorists could use self-driving vehicles for attacks. The t-test result in this case also shows a significant difference (t = -2.633; p = 0.013). The results, therefore, suggest that the distrustful are more fearful of new technologies, failures, and loss of control, while the confident are more open to the use of self-driving systems, but also more sensitive to the potential for misuse.

In order to get a deeper and more nuanced picture of the groups of people who distrust and trust self-driving cars, I used cluster analysis. This statistical method allowed me to group respondents into clusters based on similarities, so that I can not only examine individual opinions but also reveal underlying patterns and attitude groups. In the clustering process, I used the perceived advantages and disadvantages of self-driving technology as a grouping criterion. The reason is that these factors – such as safety, convenience, reliability, or even privacy concerns – fundamentally shape people's attitudes and have a significant impact on whether one adopts or rejects self-driving systems. The method has therefore allowed me to identify not only general opinions but also typical attitude profiles.

The results of the ANOVA table show that each of the variables included contributed significantly to the separation of clusters, confirming the relevance of the variables for clustering. The clusters that result from K-means clustering give the following pattern along the cluster-forming variables. Based on the patterns shown, we can place the cluster members under three names: **negative perception** cluster, because all potential positives are rated low and all potential negatives are rated high (92 people). Next is the **positive perception** cluster, where the opposite is true, i.e., positives are rated higher and negatives are rated lower. They are the easiest to convince to engage in self-driving technologies (74 people). There is also an intermediate cluster, the **control freaks**, who could be said to be an insecure layer, but in fact, it is not a uniform intermediate layer, as there is an outlier pattern of fear of self-driving cars failing, lack of control feedback, or that the hackers from outside could interfere with the system. All of these fears are viewed in terms of control over the system, hence, they are called **control freaks** (111 people).

Table 2 *ANOVA table*

	Cluster		Error		F	Sig.
	Mean square	df	Mean square	df		
Self-driving cars will have a positive impact on emissions	4.013	2	1.221	274	3.287	.039
Self-driving cars will have a positive impact on society	12.616	2	1.137	274	11.096	.000
Self-driving cars reduce car accidents	22.136	2	1.434	274	15.439	.000
Hackers are hacking into your car's system	91.255	2	1.204	274	75.774	.000
The self-driving car breaks down	91.756	2	.724	274	126.773	.000
Fear of new technology	83.439	2	1.296	274	64.387	.000
People lose their jobs because of it (e.g., taxi drivers)	83.861	2	1.279	274	65.542	.000
Control cannot be taken back	112.437	2	.823	274	136.628	.000
Too expensive	78.613	2	1.423	274	55.248	.000
The experience of driving is lost	74.335	2	1.374	274	54.085	.000
Lack of security of personal data	130.453	2	.979	274	133.192	.000

The distribution is not even, with a very high number of respondents interested in the control, with nearly a quarter of respondents in favour, and roughly a third against. In other words, nearly 40% of respondents who could be persuaded to use self-driving technologies may be able to trust it, but are not yet confident. In the following, I examine the clusters formed along the lines of attitudes towards the use of self-driving technologies in combat.

As can be seen in Figure 2, there are differences between the clusters in terms of the exploratory variables, which I compared pairwise using a partial independent samples t-test to check whether they are significant. When comparing the negative and positive perception groups, the Levene test showed that the equal variance condition was met for several variables. As for the Communication between drivers and pedestrians (F = 0.749; p = 0.388), the Need for legal regulation of self-driving cars (F = 0.299; p = 0.586), and demographic factors – age (F = 0.335; p = 0.564), place of residence (F = 0.417; p = 0.519), and education (F = 0.244; p = 0.622) – the "equal variances assumed" principle held, i.e., the variance of the responses of the two groups did not differ significantly. This suggests that the responses to these questions were relatively uniform regardless of the level of perception, or at least that there was no significant difference in the within-group variances.

In contrast, for Cybersecurity of self-driving cars (F = 7.027; p = 0.009) and Likelihood of terrorist use of self-driving vehicles (F = 6.143; p = 0.014), the difference in variances was already significant, and the "equal variances not assumed" condition had to be applied to these variables. This indicates that there was greater variation within groups on these questions – for example, there was greater variation among those with negative perceptions –, but this did not always result in significant differences between group means on the given population. This may be due to the different intensity of perceptions or the degree of uncertainty associated with perception on a given topic.

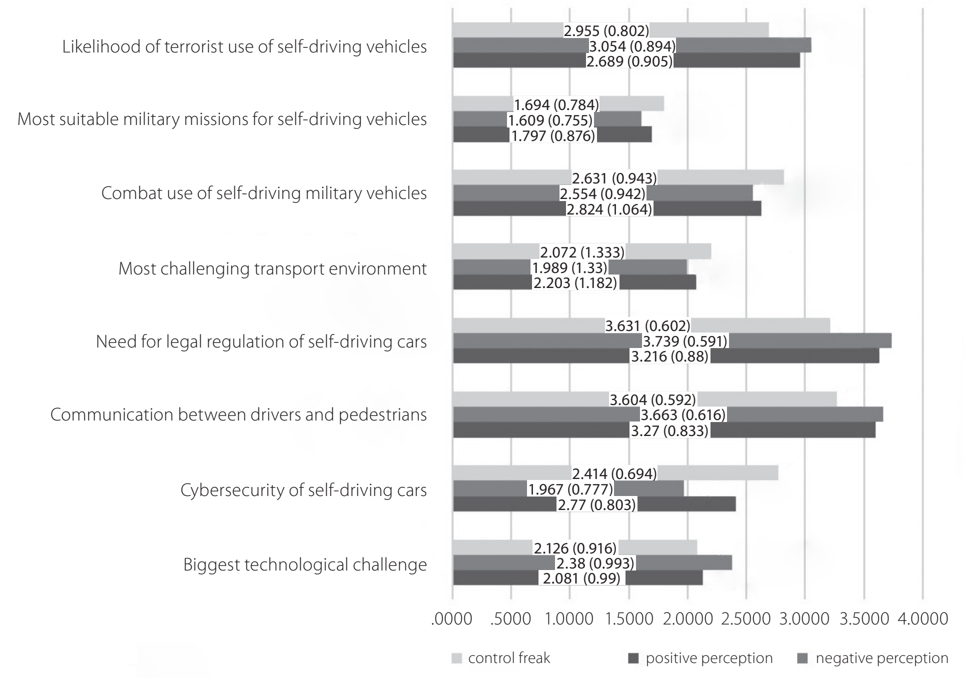


Figure 2 *Mean and Std of clusters*

Based on the results of the t-tests conducted to compare the control freak and negative perception clusters, Levene's test showed that for most of the variables tested, there was no significant difference in the within-group variances, so the condition of equal variance was met. This was also true for the variables of Communication between drivers and pedestrians (F=0.287; p=0.594), Need for legal regulation of self-driving cars (F=1.042; p= 0.310), Likelihood of terrorist use of self-driving vehicles (F=1.132; p=0.290), and Education (F=0.221; p = 0.639). This suggests that, for these factors, the opinions of the two clusters, although they may differ in content, showed a similar distribution in terms of variance, i.e., the variance of the responses did not differ significantly. However, for the variable of Cybersecurity of self-driving cars (F=5.147; p=0.025), the result "equal variances not assumed" was obtained, indicating that the variance of the responses within the clusters differed significantly for this question. This may indicate that respondents with a greater fear of loss of autonomy (control freaks) had more divergent views on the importance of cybersecurity, while the group with negative perceptions may have had a more consistent perception of risk. However, in the present population, this divergence was not always associated with a significant difference in group means. In the comparison between the control freak and positive perception clusters, the Levene test for equal variances was satisfied for the age variable (F = 23.758; p < 0.001), so the "equal variances assumed" principle was applied. The t-test result (t = -3.989; df = 201; p < 0.001) shows a significant difference between the two clusters, i.e., they differ in age: members of the control freak cluster are typically younger or older than members of the positive perception cluster. However, the difference in variances for the education variable was significantly close (F = 3.106; p = 0.080), so the "equal variances not assumed" condition was applied. The result of the t-test (t = -2.343; df = 188.687; p = 0.020) also indicates a significant difference, suggesting that there is also a difference in the level of education between the members of the two clusters, i.e., the educational background of the control freak and positive perception clusters may be statistically different.

SUMMARY

The research used a questionnaire-based approach to investigate social attitudes towards self-driving vehicles. Eight key areas were analysed: technological and transport challenges, cybersecurity, human interaction, regulatory needs, military applicability, and the potential for terrorist use. K-means clustering identified three attitude clusters: the **negative perception cluster**, which is dismissive of all technological advances but sensitive to risks; the **positive perception cluster**, which is open to self-driving technologies; and the **control freak cluster**, which is specifically concerned about loss of controllability, traceability, and control over the system. The t-test analyses showed no significant variance within clusters in several cases, such as perceptions of control or communication challenges, indicating a relative consistency of responses. However, for **cybersecurity** and the **possibility of terrorism,** there is a stronger dispersion and different patterns, especially for the negative and control-sensitive groups. Demographic factors (age, place of residence, education) did not result in significant differences in within-group variance, i.e., they did not show a prominent role in shaping perceptions. The results highlight that social trust and the management of security concerns may be key to the acceptance of technology.

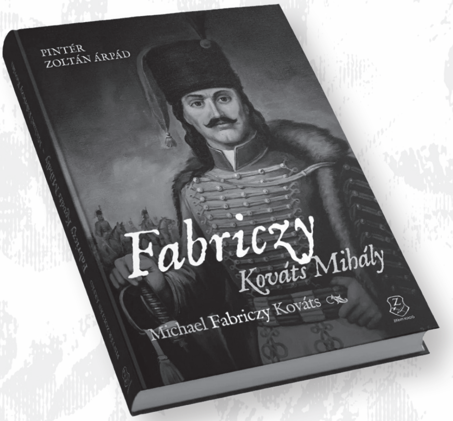
BIBLIOGRAPHY

- Atiyeh, Clifford: *Self-Driving Cars' Look, Feel Is Clearer through Final U.S. Safety Rules*. Car and Driver, 2021. https://www.caranddriver.com/news/a35247978/us-autonomous-car-safety-rules-finalized (Accessed: 01/02/2024).
- Bo, Marta: *Are Programmers In or 'Out of' Control? The Individual Criminal Responsibility of Programmers of Autonomous Weapons and Self-driving Cars*. In: Gless, Sabine – Whalen-Bridge, Helena (eds.): Human-Robot Interaction in Law and its Narratives: Legal Blame, Criminal Law, and Procedure. Cambridge University Press, 2022.
- Borenstein, Jason – Herkert, Joseph R. – Miller, Keith W.: *Self-Driving Cars and Engineering Ethics: The Need for a System Level Analysis*. Science and Engineering Ethics, Vol. 25, No. 2 (2019), 383–398. DOI: 10.1007/s11948-017-0006-0.
- Brooke, Lindsay: *U.S. DoT chooses SAE J3016 for vehicle-autonomy policy guidance*. Automotive Engineering, 2016. https://www.sae.org/news/2016/09/us-dot-chooses-sae-j3016-for-vehicle-autonomy-policy-guidance?gad_source=1&gad_campaignid=22563476365&gbraid=

0AAAAAqQfg6uFuTdv0F_vKmDueK6_OX_-l&gclid=EAIaIQobChMI9ZfNuYSojQMVzK-WDBx0weAHZEAAYAyAAEgJ_hfD_BwE&gclsrc=aw.ds (Accessed: 20/01/2023).

- Cavoli, Clemence – Phillips, Brian – Cohen, Tom – Jones, Peter: *Social and behavioural questions associated with Automated Vehicles: A Literature Review*. UCL Transport Institute, 2017.
- Chougule, Amit – Chamola, Vinay – Sam, Aishwarya – Yu, Fei Richard – Sikdar, Biplab: *A Comprehensive Review on Limitations of Autonomous Driving and Its Impact on Accidents and Collisions*. IEEE Open Journal of Vehicular Technology, Vol. 5, 2023, 142–161. DOI: 10.1109/OJVT.2023.3335180.
- Gál, István – Hima, Zoltán – Tick, Andrea: *Az autóipari termelés kockázatainak csökkentése*. Biztonságtudományi Szemle, Vol. 6, No. 1 (2024), 27–40. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/440.
- Gogoll, Jan – Müller, Julian F.: *Autonomous Cars: In Favor of a Mandatory Ethics Setting*. Science and engineering ethics, Vol. 23, No. 3 (2017), 681–700. DOI: 10.1007/s11948-016-9806-x.
- Goodall, Noah: *Ethical Decision Making During Automated Vehicle Crashes*. Transportation Research Record, No. 2424, 2014, 58–65. DOI: 10.3141/2424-07.
- Howard, Daniel – Dai, Danielle: *Public Perceptions of Self-driving Cars: The Case of Berkeley, California*. 93rd Annual Meeting of the Transportation Research Board, Washington, D.C., 2014.
- Jaradat, Maram – Jibreel, Manal – Skaik, Huda: *Individuals' perceptions of technology and its relationship with ambition, unemployment, loneliness and insomnia in the Gulf*. Technology in Society, Vol. 60 (101199), 2020. https://doi.org/10.1016/j.techsoc.2019.101199.
- Kettles, Nathan – Van Belle, Jean-Paul: *Investigation into the Antecedents of Autonomous Car Acceptance using an Enhanced UTAUT Model*. International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), Winterton, South Africa, 2019, 1–6.
- Kovács, Gábor – Hőgye-Nagy, Ágnes – Kurucz, Győző: *Human Factor Aspects of Situation Awareness in Autonomous Cars – An Overview of Psychological Approaches*. Acta Polytechnica Hungarica, Vol. 18, No. 7 (2021), 7–24. DOI: 10.12700/APH.18.7.2021.7.1.
- König, Michael – Neumayr, Lambert: *Users' resistance towards radical innovations: The case of the self-driving car*. Transportation Research Part F: Traffic Psychology and Behaviour, Vol. 44, 2017, 42–52. https://doi.org/10.1016/j.trf.2016.10.013.
- Kumar, Narender: *Use of Modern Technology to Counter Terrorism*. Centre for Internal and Regional Security, 2019.
- Kyriakidis, Miltos – Happee, Riender – de Winter, Joost: *Public opinion on automated driving: Results of an international questionnaire among 5000 respondents*. Transportation Research Part F: Traffic Psychology and Behaviour, 32, 2015, 127–140. DOI: 10.1016/j.trf.2015.04.014.
- Li, Zehua – Niu, Jiaran – Li, Zhenzhou – Chen, Yukun – Wang, Yang – Jiang, Bin: *The Impact of Individual Differences on the Acceptance of Self-Driving Buses: A Case Study of Nanjing, China*. Sustainability, Vol. 14, No. 18 (2022), 11425.
- Othman, Kareem: *Investigating the Influence of Self-Driving Cars Accidents on the Public Attitude: Evidence from Different Countries in Different Continents*. 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), 2023. DOI: 10.1109/ICSSIT55814.2023.10061032.
- Perger, Ádám: *Potential Targets of Cyber-Attacks: Legal Regulation of Drones and Self-Driving Cars*. Journal of Law and Social Sciences, No. 7 (2022), 46–52.
- Servin, Christian – Kreinovich, Vladik – Shahbazova, Shahnaz Nadir: *Ethical Dilemma of Self-Driving Cars: Conservative Solution*. In: Recent Developments and the New Directions of Research, Foundations, and Applications. Selected Papers of the 8th World Conference on Soft Computing, Springer Nature, Switzerland, II, 2023, 93–98. DOI: 10.1007/978-3-031-23476-7_9.

- Schoettle, Brandon – Sivak, Michael: *Motorists' Preferences for Different Levels of Vehicle Automation*. Sustainable Worldwide Transportation, University of Michigan, 2016.
- Szatmáry, Rozália – Lazányi, Kornélia: *Are Self-driving Cars a Safer Solution?* In: Critical Infrastructure Protection in the Light of the Armed Conflicts, Springer Nature, Switzerland, 2022, 443–455.
- United Nations: Vienna Convention on Road Traffic, 1968.
- Viktor, Patrik – Fodor, Mónika: *Adapting Self-Driving Technology*. 2024 IEEE 11th International Conference on Computational Cybernetics and Cyber-Medical Systems (ICCC) 2024, pp. 000153–000158.
- Woollard, Fiona: *The New Trolley Problem: Driverless Cars and Deontological Distinctions*. Journal of Applied Philosophy, Vol. 40, No. 1 (2023), 49–64. https://doi.org/10.1111/japp.12610.



Krisztián Végh, Norbert Daruka

THE CHALLENGE OF TECHNOLOGY-ENABLED UNMANNED AIRCRAFT SYSTEMS

DOI: 10.35926/HDR.2025.1.7

ABSTRACT: *Emerging Disruptive Technologies (EDTs) are fundamentally reshaping modern warfare, particularly in the field of military defence against drones. The rapid development of unmanned systems is creating new challenges that need to be met with innovative solutions. Technologies such as artificial intelligence, quantum computing, directed-energy weapons, and cyber warfare tools can play a key role in neutralising enemy drone threats. Artificial intelligence-based sensors and decision support systems can enable rapid detection and categorisation of drones, while directed energy weapons, such as lasers and microwave systems, can provide an efficient and cost-effective solution for their destruction. In addition, information operations tools such as electronic jamming and hacker attacks can be used to disrupt or take control of autonomous systems. The integrated use of these technologies could revolutionise the way we defend against drones and enable new strategies in modern theatres of war.*

KEYWORDS: *artificial intelligence, autonomous devices and systems, defence capability*

ABOUT THE AUTHORS:

- *Krisztián Végh is a PhD student at the Ludovika University of Public Service and a senior officer at the Defence Staff Operations Directorate. (ORCID: 0000-0001-6969-968X; MTMT: 10096868)*
- *Norbert Daruka (PhD) is the branch head of the Scientific Research Centre of the HDF Transformation Command. (ORCID: 0000-0002-7102-1787; MTMT: 10039981)*

INTRODUCTION

Europe's security environment is fundamentally shaped and influenced by the Russo-Ukrainian War, illegal migration, the potential for a parallel influx of terrorism, and, more broadly, by the conflicts in the Middle East. The lessons learned and conclusions drawn from these armed conflicts have a direct or indirect impact on the direction of domestic training and research and development. It is imperative that these lessons learned at the national level are brought into line with NATO's thinking in order to ensure that the policy developed by the Alliance can be properly supported.

The Russo-Ukrainian War brought to the surface a series of phenomena that had already been forgotten during the peace support operations of the past decades, such as the issue of extensive minefields[1] or the large-scale, planned attacks against critical infrastructure[2]

[1] Csurgó et al. 2024.

[2] Kovács 2024.

serving the population of the target country. Perhaps the most striking phenomenon of the ongoing armed conflicts is the emergence of the mass use of drones. They can be encountered in almost any type of military activity, and nations have accordingly begun to examine how they can be integrated into their own systems. It is also a natural and everyday issue that the web reports daily on successful drone attacks against armoured targets, naval vessels, and personnel as well.

THE EDT AND NATO

Technological progress has always shaped the characteristics of warfare, from the invention of gunpowder to the advent of nuclear weapons. However, the 21st century is seeing innovation on a scale and at a speed previously unimaginable. Rapid advances in artificial intelligence, robotics, biotechnology, quantum computing, and the potential of cyberspace are radically transforming the way we think about threats and the military strategies and weapons systems that respond to them. However, these 'disruptive technologies' not only pose new types of serious threats to international peace and security, but also offer new opportunities for shaping the warfare of the future.

In the coming years, and even within a decade, given the pace of development, the evolution of advanced military technologies will be shaped by four basic overarching characteristics: the rise of increasingly intelligent, interconnected, decentralised, and digital solutions. As a consequence of these trends, future military systems will increasingly operate autonomously, be interconnected in close networks, be able to operate in multiple operational environments (i.e., land, air, sea, cyber, and space) simultaneously, and perform their missions with extreme precision.

Technological innovations will increasingly become dual-use, meaning that a significant proportion of developments will come from the civilian, commercial sector and will be incorporated into military applications. This process will not only accelerate the integration of new solutions into the defence sector but will also enable their cost-effective and widespread deployment.

The emerging technology-enabled capabilities will contribute significantly to the effectiveness of NATO's military operations and organisational functioning. These tools and systems already support the five key development directions set out in the Alliance's Basic Concept for Warfare:

- gaining cognitive superiority, enabling faster and more accurate decision-making;
- integrated, multi-domain defence, ensuring coordinated cooperation among various forces and operational levels;
- multidimensional command and control capabilities enabling coordinated command and control of various operational environments;
- multi-level resilience to respond and adapt rapidly to crisis situations;
- a broad sphere of influence and projection of power to ensure NATO's strategic presence and responsiveness around the world.

Despite their wide applicability, these new technologies also present a number of challenges. NATO, and therefore our country, must seriously consider the operational, interoperability (cooperation), ethical, legal, and moral issues that they raise. Innovations, therefore, not only create opportunities but also require complex problems to be solved in order to ensure that the technological advantage will truly benefit the Alliance in the not-too-distant future.

NATO's Strategic Concept 2022[3] stresses that EDTs are changing the character of conflict, increasing their strategic importance, and becoming key areas of global competition. Technological advantage will increasingly influence success on the battlefield. Accordingly, the Allies are committed to fostering innovation and increasing investment in EDT to preserve NATO's interoperability and military superiority.

The Alliance is currently focusing on nine[4] priority technology areas[5] for EDTs:

– Artificial Intelligence;
– Autonomous systems;
– Quantum technologies;
– Biotechnology and Human Enabling Technologies;
– Space technology;[6]
– High-speed systems;
– New materials and manufacturing processes;[7]
– Energy and propulsion technologies;
– Next generation communication networks.

In these areas, NATO is developing detailed plans to accelerate responsible innovation and the rapid deployment of modern technologies, improving decision-making processes and strengthening transatlantic defence and security innovation in line with the democratic values of Allies and respect for human rights.

Therefore, the Alliance aims to develop responsible, innovative, and flexible policies to address these technologies, in close cooperation with the industrial and scientific community, within national and allied frameworks.

THE IMPACT OF TECHNOLOGY ON THE MILITARY USE OF DRONES

At the end of the 20th century, we had no idea that the warfare of the next century would be radically changed by the emergence and spread of new, so-called emerging and disruptive technologies. Of course, the military operations currently underway have also made a significant contribution to this. Advances in artificial intelligence (AI), 3D printing, and autonomous systems are significantly changing the way military equipment is developed, operated, and used. This is particularly evident in the field of aerial drones – officially known as UAVs[8] – that have become key players in modern warfare. The implications of these technologies for drones are examined in more detail below.

[3] *NATO 2022 STRATEGIC CONCEPT* – Adopted by Heads of State and Government at the NATO Summit in Madrid, 29 June 2022.

[4] In 2019, only seven were in the focus of NATO.

[5] NATO/OTAN Official website 2024.

[6] See more: Edl – Szenes (eds.) 331.

[7] Ember et al. 2024.

[8] UAV: Unmanned Aerial Vehicle.

Artificial Intelligence and Automation of Decision-Making

The use of artificial intelligence is revolutionising the autonomy and responsiveness of drones. AI-equipped UAVs are capable of real-time data analysis, target recognition, and, to a limited extent, even tactical decision making. This is particularly advantageous in hostile environments where rapid response can be vital. AI-driven systems reduce the need for human intervention, which not only shortens response times but also minimizes the risk to human resources. However, this also raises ethical and legal issues, especially if the decision to destroy a target is left to machine algorithms.

3D Printing and Manufacturing Flexibility

3D printing allows drones to be manufactured quickly and cost-effectively, especially in field environments, such as those seen near the front lines in the Russo-Ukrainian War. This technology can be used to produce not only complete vehicles, but also parts and special accessories, significantly increasing operational flexibility. With 3D printing, militaries can customise a great majority of parts and equipment,[9] such as drones for a specific mission – be it reconnaissance, transport, or even attack –, and quickly replace lost or damaged assets. This technology offers a strategic advantage, especially for smaller countries or non-state actors that do not have a large military industry.

It should be noted that standard or improvised explosive devices dropped from drones have proven to be highly effective weapons in the aforementioned conflict. Their effectiveness lies in the unmanned aerial vehicle itself and its triggering device, as it ensures productivity. Additive manufacturing technology also makes it possible to assemble parts or bodies of functionally different sizes, using so-called interposable elements. This makes it possible to assemble a hand grenade fuse and a mortar shell body into a hybrid weapon that can be launched/dropped from a drone.

Autonomous Systems and Swarm Operations

The development of autonomous systems allows the coordinated cooperation of drones in the form of "swarm operations". In these operations, hundreds or even thousands of small drones can make collective decisions, communicating with each other and adapting to the environment. Autonomous swarm operations pose new challenges to the enemy, as conventional weapons are difficult to defend effectively against highly mobile, decentralised units.

Challenges and Risks

While these technologies offer significant benefits, they also carry serious risks. Drones with AI and autonomy can be the target of cyberattacks, and the consequences of a possible hack of the control system could be severe. 3D printing makes it easy to manufacture drones, even for non-state actors, such as terrorist organisations, creating new security risks.[10] In addition, the issue of autonomous decision-making raises serious legal and ethical dilemmas: who

[9] Ember 2022a; Ember 2022b.

[10] Ember 2025.

bears responsibility in the event of an attack with civilian casualties if it is carried out by an AI-controlled device?

Artificial intelligence, 3D printing, and autonomous systems are revolutionising the potential applications of military drone technology. These developments will enable faster, more efficient, and cheaper operations, but also create new risks and moral dilemmas. Future theatres of war are likely to be increasingly shaped by these technologies, and militaries will have to adapt to new realities not only from a technological but also from a strategic and ethical perspective.

THE DIVERSITY OF DRONES

In the process of examining both the Russo-Ukrainian and the Middle East conflicts, and the lessons learned from them, several aspects have come to the fore, sometimes predicting significant changes in characteristics for the future. The emergence of drones may be familiar to the UAV category, but the development of autonomous ground[11] and waterborne[12] assets is also underway.

This article focuses on the NATO Class I category.

Table 1 *Classification of drones for military and civilian use*
(based on Government Decree 38/2021 (2.2.2011) and NATO ATP-117, edited by the authors)

National		NATO		Theoretical range	Application height	Application level
Category	Take-off weight	Class	Subclass			
E	> 600 kg	Class III	HALE	No limitation	65,000 ft	Strategic
			MALE		45,000 ft	Operational
D	150–600 kg	Class II	Tactical 150–600 kg	~200 km	18,000 ft	Tactical
C	25–150 kg	Class I	Small > 15 kg	~50 km	5,000 ft	Tactical
B1, B2	4–25 kg		Mini < 15 kg	~25 km	3,000 ft	Tactical
A1, A2	< 4 kg		Micro < 2 kg	~5 km	200 ft	Tactical

Almost all the above categories play a role in the Russia-Ukraine conflict, which is not surprising given the decades-long history of military R&D in drones and autonomous systems. A study[13] on the subject found that drones have become increasingly autonomous over time and have been widely linked to other weapons systems, their emergence having a profound impact on military doctrines and organisations. In terms of their characteristics, the drones used in the Russo-Ukrainian conflict can be divided into two broad categories: military or civilian use, and single-use or reusable, in terms of their design.

Military drones are basically designed for combat use (even though many may have a non-destructive role),[14] which means that they are equipped with various protection devices

[11] Global Defence News – Army Recognition Group official website.

[12] Northrop Grumman website.

[13] Pettyjohn 2024.

[14] Kovács – Ember 2022; Ember – Kovács 2022.

and can withstand jamming and cyber activities, which makes them difficult to detect and counter effectively. The operators of such devices undergo specific training, and their replacement is a significantly time-consuming task. The preferred reusable military drones of the Russian side were initially the Orlan-10 and various versions of the Zala, while the Lancet and Shahed versions of the single-use drones are also noteworthy. The Ukrainian side preferred the Leleka-100, Furia, and PD-1 types for reusable missions, and the Switchblade 300 and Warmate for kamikaze missions. Of course, both sides have MALE[15] devices in their systems, together with Forpost and Orion on the Russian side and the infamous TB2 on the Ukrainian side.

The division between single-use and multi-use is also valid for commercially available modified so-called "FPV"[16] drones. The emergence of known devices in their current form and known use dates back to the early 2000s, mainly for use by non-state actors and certain terrorist groups.[17]

The term FPV was probably coined as an analogy for small UAVs with modified explosive devices published on popular online video-sharing sites. However, we are convinced that this type of simplification is not appropriate for a correct assessment and interpretation of the threat they pose and, for this reason, almost certainly for the design of C-UAS[18] with appropriate effectiveness. Accordingly, we also consider it important to briefly describe the division of modified drones. Among the multiple-use devices, there are those with a triggering device, capable of delivering grenades against infantry and armoured vehicles, and those capable of carrying small arms or armour-piercing devices or incendiary agents. The one-way group is made up of guided or omnidirectional cluster munitions and drones with EFP[19] charges. Also included in this group are kamikaze drones capable of carrying modified armour-piercing grenades, the so-called improvised FPV loitering munitions.

DRONE DETECTION AND IMPACTS

When examining C-UAS activities, it is essential to review the UAS[20] architecture in order to identify weak or vulnerable points when designing an effective countermeasure.

Simplified, a small category UAS consists of an operator, a remote-control device, a C2[21] link, and the UAV device and its payload. Larger systems are complemented by GCS,[22] some kind of launch platform, and MCE[23] elements. GCS and MCE consist of physical infrastructure such as trucks, containers, or buildings, usually housing the computer that runs the applications needed to run the whole system. All of this is, of course, operated exclusively by properly trained professionals.[24]

[15] MALE: Medium Altitude Long Endurance.

[16] FPV: First Person View – the operator sees what the drone "sees". Usually designed for drone competitions and aerial photography, they are significantly more powerful than conventional quadcopters.

[17] Végh 2024.

[18] C-UAS: Counter-Unmanned Aircraft Systems.

[19] EFP: Explosively Formed Penetrator.

[20] UAS: Unmanned Aircraft Systems.

[21] C2: Command and Control.

[22] GCS: Ground Control Station.

[23] MCE: Mission Control Element.

[24] See more: Joint Air Power Competence Centre 2021.

Research into the vulnerability of UAS components has been a multi-year process, and the following breakdown helps to understand the issue.[25]

Detectability

Radar visibility is measured by the RCS[26] provided by the device. For UAVs in the smaller categories, this cross-section is relatively low; the plastic materials used in their construction and the relatively low operating altitude pose additional challenges for conventional radars.

Their visibility in the IR[27] spectrum for IR detection tools, the high-temperature components of conventional propulsion systems, and the combustion products emitted during fuel combustion provide a cross-section that can be adequately detected. The electric propulsion of smaller drones makes this method more difficult, but the temperature of the drone is different from its surroundings, so IR can be a shorter-range detection method.

Going off topic, it should be mentioned that there are also examples of protection against drones in industrial installations. The above method may be a solution to eliminate safety risks.[28] The excessive bandwidth of 5G networks enables the transmission of large information-gathering data streams of high-resolution video from surveillance drones.[29]

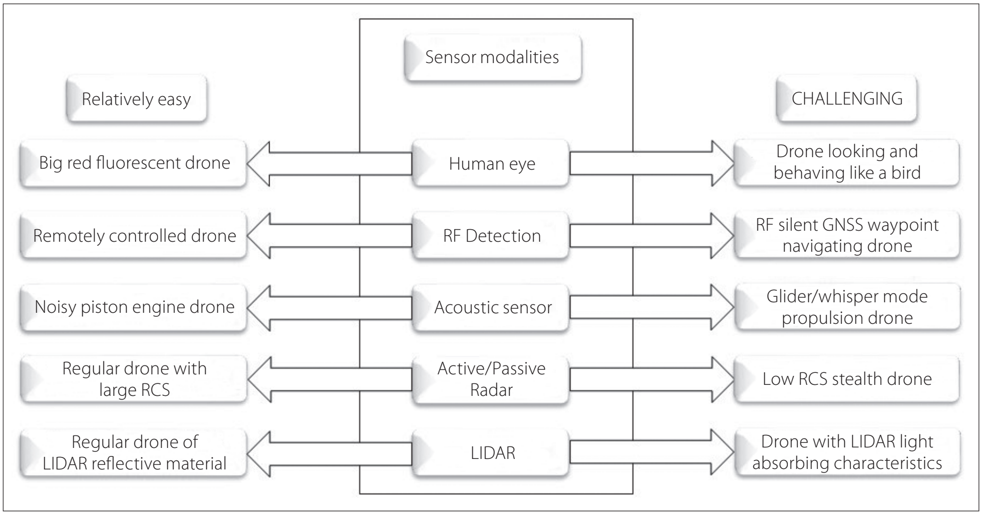

Sensor modalities
Relatively easy
CHALLENGING
Big red fluorescent drone
Human eye
Drone looking and behaving like a bird
Remotely controlled drone
RF Detection
RF silent GNSS waypoint navigating drone
Noisy piston engine drone
Acoustic sensor
Glider/whisper mode propulsion drone
Regular drone with large RCS
Active/Passive Radar
Low RCS stealth drone
Regular drone of LIDAR reflective material
LIDAR
Drone with LIDAR light absorbing characteristics

Figure 1 *Sensor modalities (based on NATO ATP-3.3.8.1, edited by the authors)*

Acoustic detection systems are usually ground-based and are used to identify the altitude and speed of the UAV. The noise level of a drone with a 70-dB sound output measured at a distance of one metre is "merged" with the roughly 20-dB sound level generated by the

[25] Haider 2021.

[26] RCS: Radar Cross-Section.

[27] IR: Infrared.

[28] Szávay – Őszi 2025.

[29] Tóth 2025.

environment at a distance of about 300 metres, which can therefore mask the drone's presence from human hearing. Acoustic detection of smaller devices is therefore of very low effectiveness and may only be suitable for shorter distances.

The effectiveness of visual detection depends largely on the size and colour of the target object and the general atmospheric and weather conditions. A further challenge in visual detection of drones is the need to distinguish them from various moving objects, such as birds or even a plastic bag caught in the wind. A drone is most likely to be heard before it is detected, and typically, the noise of a nearby drone triggers visual recognition.

Of course, there are other detection options in addition to the methods and tools briefly described above, but our aim is to raise awareness of the complexities and challenges of the detection itself. In short, C-UAS cannot rely solely on one solution, it must range from building situational awareness of personnel based on visual and acoustic detection to the use of radio frequency and laser detection techniques.

Effectors

The C-UAS technology spectrum is extremely diverse and is constantly evolving in response to the complexity and diversity of threats. The counter-technologies currently in use can be broadly grouped into five main categories: radio frequency (RF) jamming, attacks against GNSS,[30] kinetic devices, directed energy weapons (laser-based systems), and high-power microwave weapons.

The purpose of RF jamming is to interrupt the communication between the drone and the operator, typically over Wi-Fi or other freely available bands. GNSS jamming or its more sophisticated form, spoofing, can mislead the UAVs by undermining navigation capabilities by communicating false coordinates. Kinetic countermeasures, such as machine guns or even missile systems, aim at their physical destruction, but their use is almost impossible in urban or civilian environments.

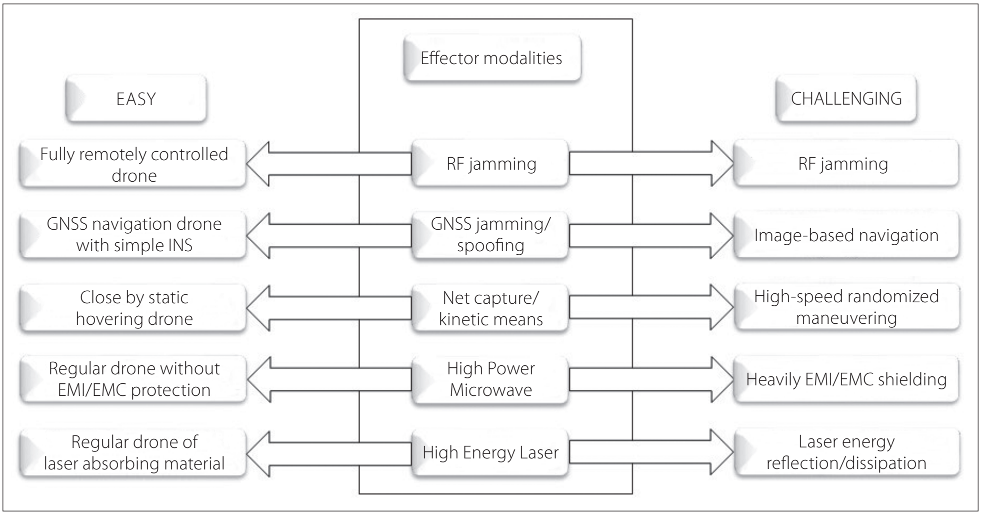

Effector modalities
EASY
CHALLENGING
Fully remotely controlled drone
RF jamming
RF jamming
GNSS navigation drone with simple INS
GNSS jamming/ spoofing
Image-based navigation
Close by static hovering drone
Net capture/ kinetic means
High-speed randomized maneuvering
Regular drone without EMI/EMC protection
High Power Microwave
Heavily EMI/EMC shielding
Regular drone of laser absorbing material
High Energy Laser
Laser energy reflection/dissipation

Figure 2 *Effector modalities (based on NATO ATP-3.3.8.1, edited by the authors)*

[30] GNSS: Global Navigation Satellite System.

Advanced laser weapons can use concentrated energy to cause structural damage to a target in a short time, while high-energy microwave systems can destroy UAV onboard systems by electronic overload. The practical application of these directed energy weapons is currently also primarily understood in a military context. In summary, the effective use of anti-drone systems requires an integrated approach combining electronic, kinetic, and informatics tools according to the level and location of the threat.

THE ROLE OF EDT IN C-UAS

The rapid proliferation of UAVs poses new challenges for organisations responsible for airspace security, or even for the military. Sensor technologies for detecting and neutralising drones, such as visual, acoustic, radio frequency (RF), radar, and LIDAR[31] systems, play a key role in addressing these threats. The integration of artificial intelligence (AI) into these systems could bring significant improvements in the effectiveness of drone detection and identification.

AI-Enabled Sensors

AI-based computer vision technologies play a prominent role in the analysis of visual sensors, the image data collected by cameras. AI can detect and track drones in real time, even against complex backgrounds. For example, DroneOptID is an AI-based software[32] that enables real-time drone detection, identification, and tracking, using optical sensors.

Acoustic sensors, RF sensors, and AI can detect the presence of drones by analysing the distinctive sound patterns emitted by the drones. By processing these sound patterns in real time, AI algorithms can increase the accuracy of detection and reduce the number of false alarms. In one study, AI-based methods have been used to efficiently classify drones with an accuracy of up to 90% by processing both radio frequency and acoustic signals.[33]

Combining data from different sensors, called sensor fusion, increases the reliability and accuracy of detection. AI algorithms can integrate and analyse this heterogeneous data, providing a more comprehensive picture of drone movements and behaviour. “Dedrone-Tracker.AI” is an AI-powered combined system that uses radio frequency, radar, imagery, and acoustic sensors to efficiently detect and track drones. The AI can analyse these signals in real-time, identifying the type of drone and pinpointing its position, filtering out UAVs identified as friendly.[34]

AI and LIDAR technology use laser beams to map the environment, creating an accurate 3D image. By analysing this data, AI can identify drones and distinguish them from other flying objects. Although LIDAR-based drone detection is still evolving, the integration of AI holds promising potential.

Integrating AI into drone detection sensors will significantly increase their efficiency and reliability. The combination of different sensor technologies and AI will enable more accurate and faster detection, identification, and tracking of drones. Integration brings many

[31] LIDAR: Light Detection and Ranging.

[32] AI-Powered Optical Detection, Identification, and Tracking Software. Drone Shield Limited.

[33] Frid et al. 2024.

[34] AXON – Dedrone official website.

benefits, but also faces challenges. Data quality, the need for real-time processing, and the reliability of AI models are key factors. Future research should focus on these challenges.

AI-Assisted Effectors

In UAV defence, not only detection but also neutralisation of targets – i.e., the use of effectors – is key. The rise of artificial intelligence opens up the possibility to significantly increase the effectiveness of various soft-kill and hard-kill systems. AI can improve reaction times, identify attack patterns, and automate decision-making. The integration of the main effector types with AI is discussed below.

Radio Frequency jamming is the disruption of communication channels between drones and their controllers, causing drones to become uncontrollable, which can force them to land or return. The effectiveness of RF jamming depends on the control frequency of the drone and the strength of the jamming signal. The integration of AI may include efficiency-enhancing directions such as identifying drone communication protocols in real time, even if they are cryptic or operate at variable frequencies (frequency hopping), or even dynamically optimizing the jamming strategy by considering the environmental spectrum usage and the target's response reactions. It is important to note, however, that RF interference is not selective and can therefore affect other communication systems.

Drone navigation systems often rely on global satellite navigation systems. In GNSS or GPS jamming, navigation signals are blocked, while in deception, false signals are transmitted, which can give the drone incorrect position information, causing it to be diverted or forced to land.

AI significantly increases the accuracy, adaptability, and effectiveness of these techniques. In the case of jamming, AI can analyse the radio spectrum in real time, detect the presence and type of GNSS signals, and optimise jamming power and frequency accordingly. In spoofing, AI can predict the target drone's movements using predictive modelling and then match them to generate credible-looking false navigation signals, avoiding detection by the target system. It also allows automatic target classification, priority management, and coordinated mass attacks, such as against drone swarms. Artificial intelligence thus not only improves the accuracy of jamming and deception but also provides adaptive, energy-efficient, and scalable operation for modern drone defence systems.

Hard-kill devices – such as machine guns, missiles, interceptors, or high-energy weapons (e.g., laser, microwave) – destroy drones in a direct physical way. AI can significantly enhance their effectiveness in target identification, tracking, target prioritisation, and fire control.

AI-based image processing algorithms can distinguish drones from other flying objects in real time, even in complex environmental conditions. Machine learning can adapt to the rapid and unpredictable movement patterns of drones, enabling precise target tracking. In multi-target situations, the system can prioritize threats with the support of AI, neutralizing the most dangerous ones first. By extending automation, autonomous weapon systems can be developed that identify and destroy targets without human intervention. But this raises serious ethical and legal questions: for example, who is responsible for the damage caused by a misidentification, and is it right for a machine to decide whether to take a human life? In the face of these moral dilemmas, it is becoming increasingly accepted that, in AI-supported systems, humans should have ultimate control over the command to fire. AI thus complements, rather than replaces, human decision-making, which is a key consideration, especially in the use of hard-kill tools.

SUMMARY

The rapid development of drone technology and the massive and often unpredictable use of unmanned systems nowadays pose a major challenge to modern warfare, especially in Europe's security environment. The conflict in Ukraine and other regional crises have clearly demonstrated that small, cheap, often commercially sourced drones can have a strategic impact. Confronted with this threat, Europe is facing an increasingly urgent need for modern, effective, and adaptive drone deterrence solutions. Detection, identification, and tracking are key elements of drone defence, for which a variety of sensor technologies are available. The performance of these sensors is significantly enhanced by artificial intelligence. Through machine learning, systems can distinguish drones more accurately from other flying objects, recognise patterns of behaviour, predict their movements, and manage mass target detection and tracking. Soft-kill devices, such as RF jamming, GNSS jamming, and spoofing, interfere with the drone's guidance or navigation. In these cases, the use of AI enables adaptive, targeted, and energy-efficient intervention: the system can map the spectrum situation in real time, pre-model the drone's behaviour, and optimise jamming or spoofing tactics accordingly. Hard-kill methods – such as net throwers, missiles, high-energy lasers, and microwave weapons – have a direct physical effect on the target. AI supports these systems in target identification, tracking, fire control, and threat prioritisation. It also brings to the fore the issue of automation, which raises moral and legal challenges. While autonomous weapons systems can be effective, the international community is increasingly advocating a human-in-the-loop approach, whereby humans have the final decision on the use of lethal force. Future anti-drone systems will certainly work in even closer integration with artificial intelligence. These systems will employ adaptive, networked, real-time decision support solutions that can adapt to dynamically changing threats. The application of AI in the areas of autonomous drone swarm protection, spectrum management, predictive threat analysis, and system cost optimisation will become inevitable. In sum, the future of drone threat protection depends on the deep integration of technological innovation and AI, but this must be done within a strict ethical, legal, and strategic framework.

BIBLIOGRAPHY

- AXON – Dedrone official website: https://www.dedrone.com/ (Accessed: 07/04/2025).
- Csurgó, Attila – Kállai, Ernő – Zsóri, Ferenc: *Az orosz műszaki tevékenység jellemzői az orosz–ukrán háborúban*. Honvédségi Szemle, Vol. 152, No. 3 (2024), 33–45. https://kiadvany.magyarhonvedseg.hu/index.php/honvszemle/article/view/1198 (Accessed: 09/04/2025).
- Edl, András – Szenes, Zoltán (eds.): *Új űrkorszak kapujában. A világűr biztonsági és katonai kérdései*. Zrínyi Kiadó, Budapest, 2024, p. 331., ISBN 978 963 327 965 6.
- Ember, István (2022a): *3D nyomtató alkalmazási lehetősége egyes speciális robbantási feladatoknál*. In: Daruka, Norbert (szerk.): Fúrás-Robbantástechnika Nemzetközi Szimpózium Különkiadás 2022. Magyar Robbantástechnikai Egyesület, Budapest, 2022, 75–83. (Accessed: 02/04/2025).
- Ember, István (2022b): *Hatásvizsgálati robbantás kumulatív töltetekkel*. Műszaki Katonai Közlöny, Vol. 32, No. 3 (2022), 13–23. Online: https://doi.org/10.32562/mkk.2022.3.2 (Accessed: 02/04/2025).
- Ember, István: *The Possible Impact of the Proliferation of 3D Printers on the Protection of Critical Infrastructure*. Advanced Sciences and Technologies for Security Applications (ASTSA), 2025, 303–312. DOI: https://doi.org/10.1007/978-3-031-78544-3_24 (Accessed: 10/04/2025).

- Ember, István – Kovács, Zoltán: *Mini drónok lehetséges alkalmazása tűzszerész műveletekben*. Haditechnika, Vol. 56, No. 2 (2022), 16–23. DOI: 10.23713/HT.56.2.04 (Accessed: 10/04/2025).
- Ember, István – Kovács, Zoltán – Vég, Róbert – Dénes, Kálmán – Daruka, Norbert: *Additive Use of Special Materials in the Military*. Scientific Bulletin, Vol. 29, No. 2 (2024), 247–255. DOI: 10.2478/bsaft-2024-0026 (Accessed: 01/04/2025).
- Frid, Alan – Ben-Shimol, Yehuda – Manor, Ezer – Greenberg, Shlomo: *Drones Detection Using a Fusion of RF and Acoustic Features and Deep Neural Networks*. Sensors, Vol. 24, No. 8 (2024). https://www.mdpi.com/1424-8220/24/8/2427?utm (Accessed: 09/04/2025).
- Global Defence News – Army Recognition Group official website: *BAE Systems Australia pioneers the future of warfare with new ATLAS CCV UGV*. 2024. https://armyrecognition.com/news/army-news/army-news-2024/bae-systems-australia-pioneers-the-future-of-warfare-with-new-atlas-ccv-ugv (Accessed: 02/04/2025).
- Haider, Andre: *The Vulnerabilities of Unmanned Aircraft System Components*. In: A Comprehensive Approach to Countering Unmanned Aircraft Systems. Germany, 2021. https://www.japcc.org/chapters/c-uas-the-vulnerabilities-of-unmanned-aircraft-system-components/?utm_source=chatgpt.com (Accessed: 09/04/2025).
- Joint Air Power Competence Centre: *A Comprehensive Approach to Countering Unmanned Aircraft Systems*. Germany, 2021. https://www.ulib.sk/files/english/nato-library/collections/monographs/japcc-books/a-comprehensive-approach-countering-unmanned-aircraft-systems.pdf (Accessed: 09/04/2025).
- Kovács, Ferenc: *A kritikus infrastruktúra stratégiai szerepe az orosz–ukrán háborúban*. Hadtudomány, Vol. 34, No. 3 (2024). https://ojs.mtak.hu/index.php/hadtudomany/issue/view/1464/1042 (Accessed: 31/03/2025).
- Kovács, Zoltán – Ember, István: *Landmine Detection with Drones*. Revista Academiei Fortelor Terestre, Vol. 27, No. 1 (2022), 84–92. https://www.armyacademy.ro/reviste/rev1_2022/Kovacs.pdf (Accessed: 09/04/2025).
- *NATO 2022 STRATEGIC CONCEPT*. Madrid, 29 June 2022. https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf (Accessed: 01/04/2025).
- NATO/OTAN Official website: *Emerging and disruptive technologies*. 2024. https://www.nato.int/cps/bu/natohq/topics_184303.htm (Accessed: 01/04/2025).
- NATO STANAG 2663 Countering Class I Unmanned Aircraft Systems (UAS) Doctrine.
- Northrop Grumman website: *Manta Ray*. https://www.northropgrumman.com/what-we-do/sea/manta-ray (Accessed: 02/04/2025).
- Pettyjohn, Stacie: *Evolution Not Revolution. Drone warfare in Russia's 2022 Invasion of Ukraine*. Center for a New American Security, 2024. https://www.cnas.org/publications/reports/evolution-not-revolution (Accessed: 01/04/2025).
- Szávay, István – Őszi, Arnold: *Protection Management Against Drones in Industrial Facilities*. Advanced Sciences and Technologies for Security Applications (ASTSA), Springer, Cham, 2025, 661–672. DOI: https://doi.org/10.1007/978-3-031-78544-3_53 (Accessed: 09/04/2025).
- Tóth, András: *Military 5G as a Critical Information Infrastructure*. Advanced Sciences and Technologies for Security Applications (ASTSA), Springer, Cham, 2025, 723–731. DOI: https://doi.org/10.1007/978-3-031-78544-3_57 (Accessed: 09/04/2025).
- Végh, Krisztián: *A repülő IED, mint harctéri innováció* (Flying IEDs as Tactical Innovations). In: Daruka, Norbert – Ember, István – Kovács, Zoltán Tibor (szerk.): III. Fúrás-robbantástechnika nemzetközi szimpózium különkiadás 2024. Magyar Robbantástechnikai Egyesület, Budapest, 2024, 80–93. https://m2.mtmt.hu/gui2/?mode=browse&params=publication;35463363 (Accessed: 03/04/2025).

HDR 2025, Nr. 1, 92–103.

Tamás Kun

GEOPOLITICAL TENSIONS AROUND THE HORN OF AFRICA

DOI: 10.35926/HDR.2025.1.8

ABSTRACT: *The Red Sea crisis has significantly altered cargo routes in maritime transport, resulting in a ten percent increase in shipping costs and several days longer transportation times. Around the Horn of Africa, several attacks occurred that were carried out by Houthi rebels from Yemen. The Iran-backed group uses these attacks as a form of message to the United States and its allies, showing sympathy for Gaza in the Israel-Hamas War. The neighbouring Djibouti had to reinforce its coast guard patrols to ensure security and respond to the rising tensions in the area. The paper examines the situation in the Gulf of Aden and the Red Sea, analysing the possible reasons behind the strikes against vessels and other targets in the region, where all members of the "Four Policemen" were present in the arrangement of the conflict.*

KEYWORDS: *Red Sea crisis, maritime transport, proxy war, international security system*

ABOUT THE AUTHOR:

Tamás Kun, PhD candidate, Óbuda University, Doctoral School on Safety and Security Sciences (ORCID: 0000-0002-6620-7157; MTMT: 10069630).

INTRODUCTION

The Four Policemen was a postwar concept and the messenger of the United Nations after World War II, where the United States, the United Kingdom, the Soviet Union, and China came together as guarantors of peace in the world. In President Franklin D. Roosevelt's vision, these nations would provide security by overseeing activities through their sphere of influence.[1] This concept influenced world affairs for roughly 75 years. After the Cold War, major powers fought for dominance in trade, the United States' hegemony had shrunk from its former glory, compared to it taking up about half of the globe's GDP alone after WWII. After several incidents, the USA made a proposal to its allies in order to establish an alliance to counter the rising threats. Secretary of Defense Lloyd Austin announced Operation Prosperity Guardian in December 2023. At the start of the year, CNN reported on US and UK strikes in response to the Iran-backed Houthi attacks. Western powers transferred serious capabilities in the region to support Israel. Both in traditional and social media, some reports often mention the connections between the Hamas-Israeli War and the Red Sea crisis. The **international security system** (ISS) is going through a vivid transformation, where these new proxy wars are milestones along the way.

[1] Miscamble 2009.

THE COLLAPSE OF THE ISS AND THE MILITARY RESPONSES FROM MAJOR POWERS

Transportation of goods via sea is a crucial point in international trade and the extension of power, which was a key element in the US military doctrine for decades after the Second World War. In this field, a potential rival is China, which is actively seeking opportunities to challenge the USA and trying to acquire dominance in trade. These issues have the potential to make further impact on the affected parties, where economic and humanitarian crises are already on the table. Maritime shipping is key to getting the primary position in global trade, since most of the goods are transported via sea shipping.

Robert Tucker wrote[2] in 1980 that "It is the Gulf that forms the indispensable key to the defense of the American global position, just as it forms the indispensable key without which the Soviet Union cannot seriously aspire to global predominance."[3] In military performance, to be a global player, a nation state must have the ability to control sea operations. International terrorism was also a key problem[4] in the region. After the arms embargo in 1992, the international community believed that the threat had been stopped at least in the Horn.[5] In 2008, piracy in the Gulf of Aden region accounted for 37 percent of all reported piracy activities.[6] In the 2000s, Somali pirates were very active,[7] which sparked similar international cooperation as we see today. The Djibouti Code of Conduct included actions to repress piracy activities in the Indian Ocean and the Gulf of Aden.[8] Djibouti is a strategic location for the major military powers in the world.

On 19 October 2023, Yemen's Houthis launched missiles and drones at Israel, demanding the end of the conflict in the Gaza Strip. Later on, this act led to the Red Sea crisis. After months of attacks on Red Sea shipping targets, the USA and the UK launched airstrikes against Houthi targets across Yemen.[9] Houthi sources claimed that they had attacked a US warship, however, they could not provide evidence for it.[10] Among the European allies, the US involvement in the Israel-Hamas conflict was not welcomed at first, nor were the strategic goals of **Operation Prosperity Guardian**. However, on 19 February 2024, the EU also launched its maritime security operation named **Operation Aspides**. In order to counter the rising threat in the Red Sea, the Indian Ocean, and the Persian Gulf, the EUNAVFOR mission started its activity to protect and safeguard commercial vessels in the region.[11] A popular phrase is circulating in the comments section on YouTube, saying, "Yemen has the right to defend itself." There is competition between superpowers and regional powers for the control of ports, which might lead to war at a point because of the rising foreign military presence around the Horn of Africa.[12] In March 2021, the Chinese-owned Ever Given container ship blocked the Suez Canal for six days. This accident highlighted the

[2] Tucker 1980.

[3] Aliboni 1985.

[4] Besenyő 2023.

[5] Besenyő – Sinkó 2022.

[6] Chalk 2009, 2.

[7] Shortland – Vothknecht 2011.

[8] Kraska – Wilson 2009.

[9] Stewart et al. 2024.

[10] Gambrell 2024.

[11] European External Action Service 2024.

[12] Ashine 2024.

weight and necessity of this trading route in the global economy.[13] The ongoing military conflict between Ukraine and Russia, as well as the unrest in the Middle East, underlined the fragility of shipping networks and supply chains. The attacks carried out by the Houthis from Yemen have redrawn commercial shipping routes, by switching from the Red Sea to the Cape of Good Hope due to geopolitical tensions in the region.[14] The old international security system, where major powers had different approaches to military activities, is under transformation. Western powers reacted by making an international alliance, led by the USA. China used its diplomatic channels to negotiate its positions. Russia used these events to engage in diplomatic clashes with its adversaries.

United States

Considering the seriousness of the circumstances, the USA did not hesitate in its response to the events. “The Red Sea is a critical waterway that has been essential to freedom of navigation and a major commercial corridor that facilitates international trade.”[15] Operation Prosperity Guardian is a multinational security initiative under the flag of the Combined Maritime Forces of ten countries: the United States, the United Kingdom, Bahrain, Canada, France, Italy, the Netherlands, Norway, the Seychelles, and Spain.[16] The USA deployed naval capabilities to the region, namely the USS Florida, a cruise missile submarine that took part in the attack on Yemen carried out in January 2024, the USS Philippine Sea, a guided missile cruiser, and two Arleigh Burke-class guided missile destroyers, the USS Gravely and the USS Mason. It also deployed aerial capabilities, including 22 fixed-wing USS Dwight D. Eisenhower aircraft carriers (Figure 1).[17]

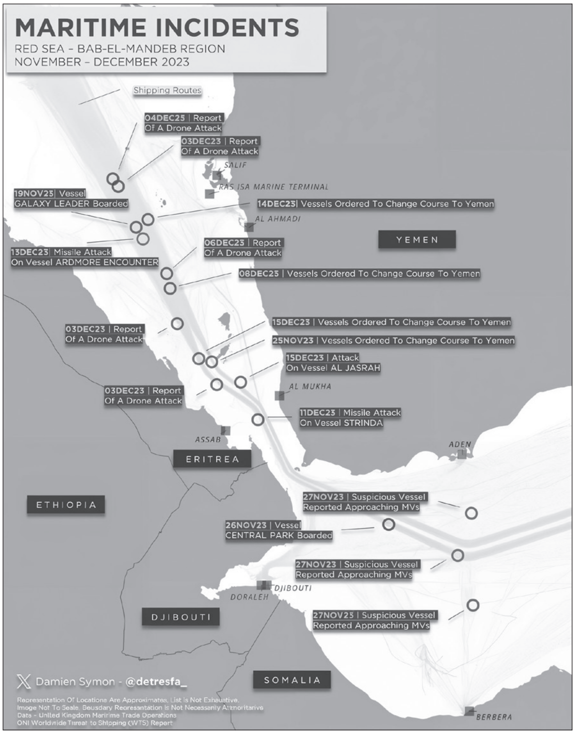

MARITIME INCIDENTS
RED SEA – BAB-EL-MANDEB REGION
NOVEMBER – DECEMBER 2023
Shipping Routes
04DEC25 | Report Of A Drone Attack
03DEC23 | Report Of A Drone Attack
SALIF
RAS ISA MARINE TERMINAL
19NOV23| Vessel GALAXY LEADER Boarded
14DEC23| Vessels Ordered To Change Course To Yemen
AL AHMADI
YEMEN
13DEC23| Missile Attack On Vessel ARDMORE ENCOUNTER
06DEC23 | Report Of A Drone Attack
08DEC25 | Vessels Ordered To Change Course To Yemen
03DEC23 | Report Of A Drone Attack
15DEC23 | Vessels Ordered To Change Course To Yemen
25NOV23 | Vessels Ordered To Change Course To Yemen
15DEC23 | Attack On Vessel AL JASRAH
AL MUKHA
03DEC23 | Report Of A Drone Attack
11DEC23 | Missile Attack On Vessel STRINDA
ASSAB
ERITREA
ADEN
ETHIOPIA
27NOV23 | Suspicious Vessel Reported Approaching MVs
26NOV23 | Vessel CENTRAL PARK Boarded
27NOV23 | Suspicious Vessel Reported Approaching MVs
DJIBOUTI
DORALEH
27NOV25 | Suspicious Vessel Reported Approaching MVs
DJIBOUTI
Damien Symon - @detresfa_
SOMALIA
Representation Of Locations Are Approximates, List Is Not Exhaustive.
Image Not To Scale. Boundary Representation Is Not Necessarily Authoritative
Data - United Kingdom Maritime Trade Operations
ONI Worldwide Threat to Shipping (WTS) Report
BERBERA

Figure 1 *Red Sea – Bab-el-Mandeb region maritime incidents*

Source: *Symon 2023*

[13] Mechai – Wicaksono 2024.

[14] Yap – Yang 2024, 121 (104004).

[15] U.S. Department of Defense 2023.

[16] Helou 2024.

[17] Liebermann et al. 2024.

United Kingdom

From November 2023 to February 2024, HMS Diamond, a Royal Navy destroyer, led the UK's maritime response to Houthi attacks. It was replaced by HMS Richmond and subsequently by HMS Duncan.[18] More than half (55%) of UK exporters reported that they had been disrupted while shipping in the Red Sea.[19] In the present, the UK provides great support for the US. The UK maintains an organization called the United Kingdom Maritime Trade Operations (UKMTO), which is an office that has experienced a significant increase in the number of incident reports. UKMTO recorded a 475 percent increase in incidents reported by seafarers in the Middle East since the attacks began in autumn 2023, with over 2,500 emails received by the HQ daily.[20] This crisis showed the UK its dependence on the United States, which is an ironic situation because in the past, the United States' key fear factor was that the British Royal Navy could be dangerous to the USA's independence.

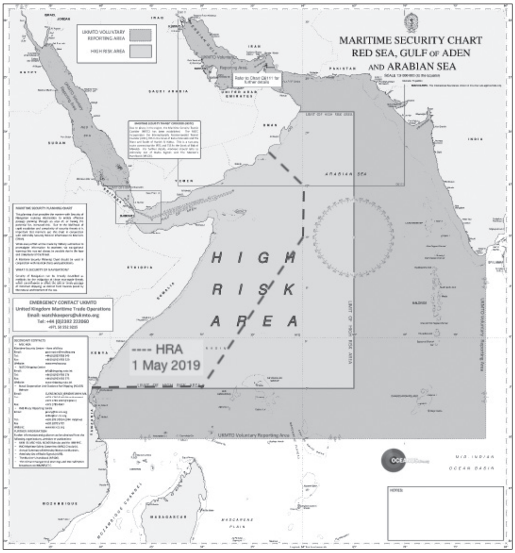


Figure 2 *IOR High Risk Area*

Source: *Oceanuslive.org 2019*

The map (Figure 2) shows a decrease in the High Risk Area (HRA). In the square, the old HRA can be seen from December 2015, and the dashed lines mark it as of 1 May 2019. As announced on 22 August 2022, the Indian Ocean HRA for piracy would be removed completely at 00:01 UTC on 1 January 2023. The area under removal, shown as the High Risk Area, can be seen in the UKHO Chart Q6099.[21] The decision was explained on the basis that piracy activities were about to drop.

Russia

In response to the escalation of military procedures in the Gaza Strip, the Ansar Allah (Houthis) movement warned that they would carry out strikes against Israeli territory and prevent ships connected to the conflict from bypassing the Bab el-Mandeb Strait. Since November 2023, the group has targeted dozens of commercial vessels in the Red Sea and the Gulf of Aden.[22] Russian officials reacted harshly to the news about the West's response to the Houthi attacks. The Kremlin's spokesman, Dmitry Peskov, said that they were 'illegitimate'. The Russian Ministry of Foreign Affairs urged a UN Security Council meeting to discuss the recent events. Ambassador Linda Thomas-Greenfield, US representative to

[18] House of Commons Library 2024, 20.

[19] BBC 2024.

[20] Royal Navy News 2024.

[21] Baltic International Maritime Council 2022.

[22] TASS 2024.

the UN, referred to Article 51 of the UN Charter, stating that response measures were taken to ensure the freedom of navigation and the free flow of commerce.[23] President Putin claimed that the new geopolitical situation supports the idea of a Northern Sea Route that runs around Russia's Arctic coastline. He also used this opportunity to promote an alternative trade route that connects Russia to the Indian Ocean via Iran.[24] The Russian Federation used these attacks as a perfect opportunity for diplomatic clashes with the West. Political interests often precede material ones because the country is rich in material resources. The Hamas-Israeli conflict provided the necessary means to engage in proxy conflict with the US. Their relationship became closer with Iran due to their 'Special military operation' in Ukraine. Also, they have broadened their cooperation with BRICS countries, further developing bilateral agreements and expanding their membership, which is now referred to as BRICS plus, counting 10 members with Iran, Egypt, Ethiopia, and the United Arab Emirates joining the group. The 15th summit of the BRICS countries was held in Johannesburg, South Africa, on 22–24 August 2023.

China

On 23 March 2024, the Houthis launched four anti-ship missiles at a Chinese-owned oil tanker in the Red Sea, regardless of the existing non-aggression agreement between the two sides. The Chinese military eventually did not intervene, based on the principle that the primary targets of the attacks were the US and its allies.[25] The current tensions around the Suez Canal are bothering Chinese investors because they have invested a lot of money in the support of the safe passage of commercial vessels.[26] From the perspective of the People's Republic of China, these events are about to make room for challenging the US trade dominance in the world. The Communist Party negotiated a deal with the Houthis that Chinese ships would remain unaffected by the Yemeni operations. However, there was a case when a Chinese-owned oil tanker was hit by anti-ballistic missiles. It could happen because there were intelligence-related issues around the ownership of the vessel. Nevertheless, it was a blow to Chinese diplomacy.

EFFECTS ON AFRICAN COUNTRIES AROUND THE HORN

Djibouti hosts several foreign military bases, which ensure the security of the Bab el-Mandeb Strait. It is in the best interest of African states to establish a forum for negotiations to mediate among major powers, as was the case during the Qatar diplomatic crisis.[27] "Port of Djibouti is the only port that adopts the International security standards for ships and ports on the Horn of Africa."[28] The continent is already facing difficult economic challenges due to the Russo-Ukrainian War, from where grain and fertilizer imports are expected. These events further deepen problems with availability and rising costs. Insurance premiums have gone up, and

[23] Thomas-Greenfield 2024.

[24] Meyer 2024.

[25] Samaan 2024.

[26] Cash 2024.

[27] Vertin 2019.

[28] Maashi 2017, 50.

longer routes block the way towards economic growth and stability.[29] For the African community, it means a harsher race for opportunities that could guarantee the background for future development. The Russo-Ukrainian War showed how an eruption in the global supply chain can affect economies all over the world. In the case of the African continent, the Black Sea Grain Initiative was a good example of how the conflict among global actors can endanger societies relying greatly on grain imports. Russia used this issue actively in its foreign policy narratives, promising tons of grain exported to African countries. Russian President Vladimir Putin promised free grain for six countries: Burkina Faso, Zimbabwe, Mali, Somalia, Eritrea, and the Central African Republic.[30]

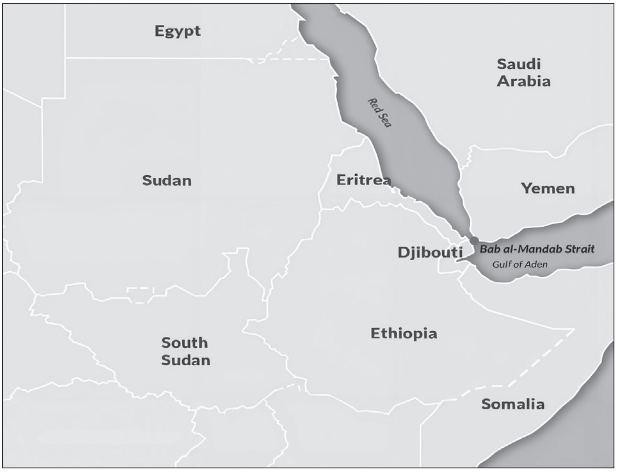


Figure 3 *The Red Sea and the Gulf of Aden*
Source: *Walker 2024*

The Bab el-Mandeb (which means "Gate of Grief" or "Gate of Tears" in Arabic) is a strait that separates Djibouti from Yemen, where the Red Sea conflict takes place. Houthi fighters have launched several rockets at Israel-related ships since November 2023. In response to the ongoing events, Djibouti reinforced its coast guard patrolling services. The country achieved serious developments in economic growth in recent years, and the ongoing crisis would threaten its results. It hosts many foreign military bases; however, Djibouti is not taking part in the US-led coalition strikes against the Houthis.[31] The events in the Red Sea and the Indian Ocean provide opportunities for piracy activities. The changed course of actions, adopted by the rest of Africa, also opened doors for new looting spots, especially when vessels must sail close to the coast.[32]

[29] Walker 2024.
[30] Heintz et al. 2023.
[31] Africanews 2024.
[32] Vreÿ – Blaine 2024.

CONSEQUENCES FOR WORLD TRADE

In the centre of the recent conflict are Yemen's Houthi rebels, who took hold of the world's highest-traffic maritime straits with the intent of supporting the Hamas war against Israel in the Gaza Strip. The Houthis' interest is to tie international actors' hands via sabotaging their supply chains in trade, similar to the situation in the 2000s with Somali piracy. However, this conflict goes beyond regional matters.[33] The Suez Canal Route takes a 10–15 percent share of global trade operations.[34] The port city of Piraeus faced a decrease in its container transport volume. In June 2024, it experienced a 10.1 percent drop in container arrivals in comparison with the 12.9 percent decline in the first half of the year. Also, Cosco-managed terminals in Spain, namely Valencia and Bilbao, reported an increasing trend with 31 percent in June and an uptrend of 13.2 percent for the first and second quarters of the year. The two terminals in Piraeus (Piers II and III) had a turnover of 366,500 TEU[35] in June, lagging behind the 407,600 TEU from the previous year, while having 1.95 million TEU in the first six months of the year compared to the 2.25 million TEU from 2023. At the Spanish terminals, they managed 344,200 TEU in June compared to the 262,800 from the previous year, and altogether 1.75 million TEU in the first half of the year compared to the 1.54 million TEU from 2023.[36] Shipping companies are about to alter their routes toward the Cape of Good Hope. This would result in longer shipping times and an increase in fuel consumption and crew time, leading to a rise in the cost of transport, which would later be passed on to customers.[37] An UNCTAD report claimed that the alternative routing could result in an additional 70 percent increase in greenhouse gas "emissions for shipping routes from Southeast Asia to Northern Europe".[38] There is a 20–30 percent increase in USD per FEU[39] rates on the four largest container shipping routes in the world. Demand peaked at a record high of 9.2 percent increase in Q1 2024 compared to the same period the previous year, at a time when there was pressure on shipping capacity due to the crisis in the Red Sea.[40]

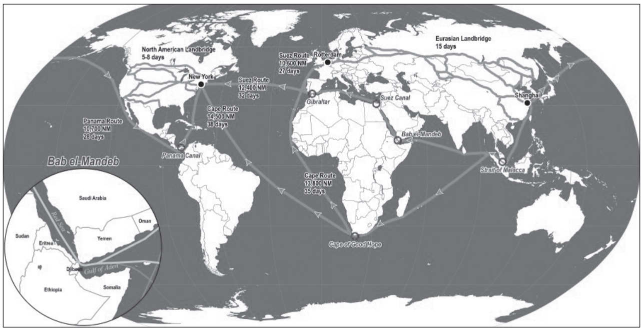


Figure 4 *Shipping routes map*

Source: *Notteboom et al. 2022*

[33] Carson et al. 2024.

[34] Ziady 2024.

[35] TEU: twenty-foot equivalent unit; term used in shipping to determine the amount of container traffic.

[36] Glass 2024.

[37] Lenderking 2024.

[38] Peng et al. 2024, 19.

[39] FEU: forty-foot equivalent unit; term used in shipping to determine the amount of container traffic.

[40] Stausbøll 2024.

On this map, we can see the traditional shipping routes. The Suez route has been sabotaged by the ongoing conflicts; an alternative to it is the Cape route, but it is eight days longer. The Russians came up with the idea of a Northern Arctic route, which is probably in their financial interest, too. The disruption in this region mostly affects European supply chains, with the Shanghai-Rotterdam line facing serious delays in the transportation of goods. This 10,600-nautical-mile-long route normally takes 27 days with a speed of 16 knots, while the alternative Cape route is considerably longer, with 13,800 nautical miles, taking 35 days with a 16-knot speed. The change in the shipping route adds an extra week to the transit time, but 10 to 14 days is more common according to the ports report. Cargo and ship insurance rates increased by 1 percent of the total cargo value compared to the general 0.1 percent level.[41] Another source claims that the route change can lead to even a 20-day delay in shipping.[42]

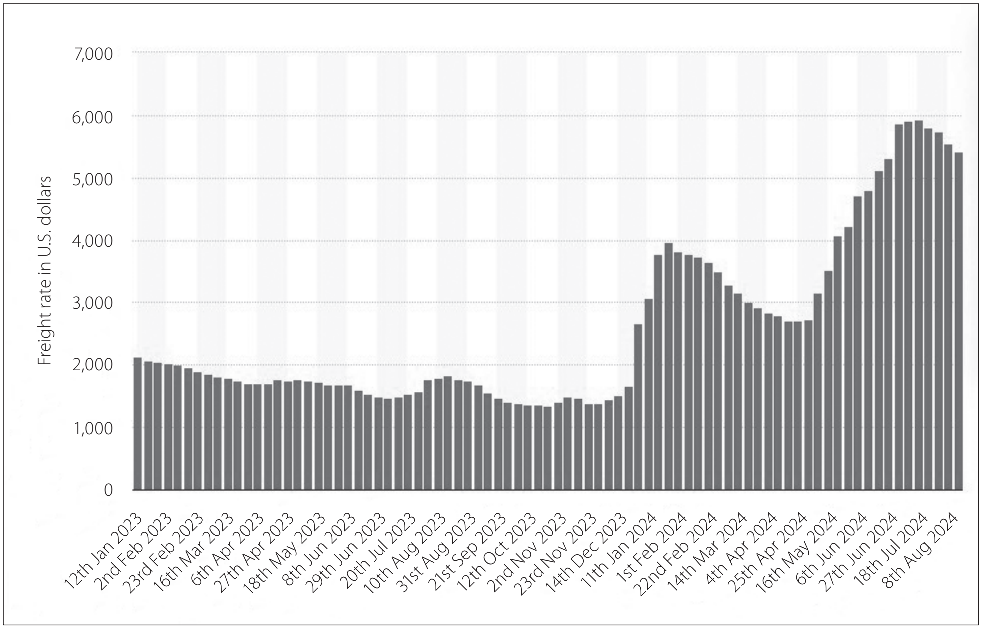


Figure 5 *Global container freight rate index from the 12th of January 2023 to the 15th of August 2024 (in U.S. dollars per 40-foot container)*

Source: *Statista.com 2024*

Data show how a container's shipping price has changed between 2023 and 2024. In the rates, we can see a spike at the start of 2024 due to tensions rising over the months after the beginning of the Hamas-Israeli war and the escalation of events, which led to insecurity in shipping. The international response from the 'Big Four' further raised the stakes, as they used the situation developed in the region for their strategic interest. Since April 2024, the cost of shipping a container has doubled, going up from USD 2,706 to USD 5,901. Shipping fares on the China–Northern Europe lane have increased by 523 percent compared to the previous year. In addition, shipping from China to the US East Coast has gone up by 246 percent.[43]

[41] Port Economics, Management and Policy 2024.

[42] Marinero 2023.

[43] Crown World Mobility 2024.

CONCLUSION

The Red Sea conflict poses serious challenges to the US dominance in the region and maybe globally, too. It is also troublesome that, at least on the narrative level, a military group is claiming an open attack against the world's most formidable military force. The forming of alliances on both sides of the conflict deepens the arrangement of the already hostile state of the current world affairs. There are visible signs of the Russian-Chinese cooperation at least on the diplomatic level, which might be seen as a prelude to the UN General Assembly voting sessions. China strategically refuses to get involved in the current matter, which can be explained by both military and commercial interests. We are already in a 'post-policeman' era as we spectate the geopolitical tensions around the Horn of Africa, which represents a choke point of foreign affairs. The Suez Canal also had key importance in both World Wars since it is a critical pathway from the Mediterranean Sea to the Indian Ocean. A new equilibrium situation is emerging that will go beyond the scope of the UN Security Council's permanent members.

BIBLIOGRAPHY

- Africanews: *Djibouti steps up coast guard patrols amidst the Red sea crisis*. 2024. [Online] Available at: https://www.africanews.com/2024/02/06/djibouti-steps-up-coast-guard-patrols-amidst-the-red-sea-crisis/ (Accessed: 07/09/2024).
- Aliboni, Roberto: *The Red Sea Region – Local Actors and the Superpowers*. Routledge, 1st Edition, London, 1985. DOI: https://doi.org/10.4324/9781315684833.
- Ashine, Surafel Getahun: *The new global superpower geo-strategic rivalry in the red sea and its implications for peace and security in the horn of Africa*. Social Sciences & Humanities Open, Vol. 9 (100834), 2024. DOI: https://doi.org/10.1016/j.ssaho.2024.100834.
- Baltic International Maritime Council: *Indian Ocean High Risk Area for piracy to be removed on 1 January*. 2022. [Online] Available at: https://www.bimco.org/insights-and-information/safety-security-environment/20221216-hra-indian-ocean (Accessed: 13/09/2024).
- BCC: *Scale Of Red Sea Disruption Revealed*. 2024. [Online] Available at: https://www.britishchambers.org.uk/news/2024/02/scale-of-red-sea-disruption-revealed/ (Accessed: 04/09/2024).
- Besenyő, János: *Somalia: A Battlefield of Intelligence Services*. In: Shaffer, Ryan (ed.): The Handbook of African Intelligence Cultures. Rowman & Littlefield, Lanham (Maryland), 2023, 601–614. DOI: https://doi.org/10.5771/9781538159989-601.
- Besenyő, János – Sinkó, Gábor: *Combating piracy strategically: Analysing the successes and challenges of NATO and EU interventions off the Somali coast*. South African Journal of International Affairs, Vol. 29, No. 3 (2022), 295–309. DOI: https://doi.org/10.1080/10220461.2022.2125064.
- Carson, Johnnie – Rondos, Alex – Stigant, Susan – Woldemariam, Michael: *The Red Sea Crisis Goes Beyond the Houthis*. Foreign Affairs, 2024. [Online] Available at: https://www.foreignaffairs.com/somalia/red-sea-crisis-goes-beyond-houthis (Accessed: 04/09/2024).
- Cash, Joe: *Explainer: Houthi attacks expose China's commercial stakes in Red Sea*. Reuters, 2024. [Online] Available at: https://www.reuters.com/world/middle-east/houthi-attacks-expose-chinas-commercial-stakes-red-sea-2024-01-15/ (Accessed: 30/08/2024).
- Chalk, Peter: *Maritime piracy: Reasons, Dangers and Solutions*. RAND Corporation, Santa Monica, 2009. [Online] Available at: https://www.rand.org/content/dam/rand/pubs/testimonies/2009/RAND_CT317.pdf (Accessed: 15/10/2024).

- Crown World Mobility: *Freight rates: is the wind finally being taken out of rate-rise sails?* 2024. [Online] Available at: https://www.crownworldmobility.com/insights/freight-rates-is-the-wind-finally-being-taken-out-of-rate-rise-sails/ (Accessed: 10/09/2024).
- European External Action Service: *EUNAVFOR Operation ASPIDES*. 2024. [Online] Available at: https://www.eeas.europa.eu/eunavfor-aspides_en?s=410381 (Accessed: 14/10/2024).
- Gambrell, Jon: *Yemen's Houthi rebels say they attacked a US warship without evidence. An American official rejects the claim*. The Associated Press, 2024. [Online] Available at: https://apnews.com/article/yemen-houthi-us-attack-red-sea-d137bfd5a328601fc0214a9ae56b4870 (Accessed: 18/10/2024).
- Glass, David: *Red Sea crisis hits volumes at port of Piraeus*. Seatrade Maritime News, 2024. [Online] Available at: https://www.seatrade-maritime.com/ports-logistics/red-sea-crisis-hits-volumes-at-port-of-piraeus (Accessed: 07/09/2024).
- Heintz, Jim – Lederer, Edith M. – Megerian, Chris – Santana, Rebecca: *Putin promises no-cost Russian grain shipments to 6 African countries*. The Associated Press, 2023. [Online] Available at: https://apnews.com/article/russia-putin-africa-summit-food-crisis-de317f5075d4b1719ade457f4eabbf82 (Accessed: 29/11/2023).
- Helou, Agnes: *Crowded waters: Who's doing what in the international hotspot of the Red Sea*. Breaking Defense, 2024. [Online] Available at: https://breakingdefense.com/2024/03/crowded-waters-whos-doing-what-in-the-international-hotspot-of-the-red-sea/ (Accessed: 20/09/2024).
- House of Commons Library: *UK and international response to Houthis in the Red Sea 2024/25*. Research Briefing, 2025. [Online] Available at: https://researchbriefings.files.parliament.uk/documents/CBP-9930/CBP-9930.pdf (Accessed: 05/09/2024).
- Kraska, James – Wilson, Brian: *Combating pirates of the Gulf of Aden: The Djibouti Code and the Somali Coast Guard*. Ocean & Coastal Management, Vol. 52, No. 10 (2009), 516–520. https://doi.org/10.1016/j.ocecoaman.2009.07.002
- Lenderking, Timothy A.: *Securing the Red Sea: A Global Response*. US Department of State, 2024. [Online] Available at: https://2021-2025.state.gov/securing-the-red-sea-a-global-response/ (Accessed: 25/08/2024).
- Liebermann, Oren et al.: *US and UK carry out strikes against Iran-backed Houthis in Yemen*. CNN, 2024. [Online] Available at: https://edition.cnn.com/2024/01/11/politics/us-strikes-houthis-yemen/index.html (Accessed: 10/08/2024).
- Maashi, Haifa Ahmed Al: *From Security Governance to Geopolitical Rivalry: Iran-GCC Confrontation in the Red Sea and the Indian Ocean*. Asian Journal of Middle Eastern and Islamic Studies, Vol. 11, No. 4 (2017), 46–63. DOI: https://doi.org/10.1080/25765949.2017.12023317.
- Marinero, James: *Operation 'Prosperity Guardian' Starts In The Red Sea*. Medium, 2023. [Online] Available at: https://medium.com/the-dock-on-the-bay/operation-prosperity-guardian-starts-in-the-red-sea-cec22152c97f (Accessed: 17/09/2024).
- Mechai, Nadhir – Wicaksono, Hendro: *Causal Inference in Supply Chain Management: How Does Ever Given Accident at the Suez Canal Affect the Prices of Shipping Containers?* Procedia Computer Science, Volume 232, 2024, 3173–3182. https://doi.org/10.1016/j.procs.2024.02.133.
- Meyer, Henry: *Russia Builds New Asia Trade Routes to Weaken Sanctions Over War*. Bloomberg, 2024. [Online] Available at: https://www.bloomberg.com/news/articles/2024-04-17/russia-builds-new-asia-trade-routes-to-weaken-sanctions-over-war (Accessed: 10/09/2024).
- Miscamble, Wilson D.: *Roosevelt, Truman and the Development of Postwar Grand Strategy*. Orbis, Vol. 53, No. 4 (2009), 553–570. https://doi.org/10.1016/j.orbis.2009.07.008.
- Notteboom, Theo – Pallis, Athanasios – Rodrigue, Jean-Paul: *Port Economics, Management and Policy*. Routledge, 1st Edition, New York, 2022. https://doi.org/10.4324/9780429318184.

- Oceanuslive.org: *Indian Ocean Piracy High Risk Area to be Further Reduced*. 2019. [Online] Available at: https://www.oceanuslive.org/main/viewnews.aspx?uid=00001272 (Accessed: 08/09/2024).
- Peng, He – Wang, Meng – An, Chunjiang: *Implied threats of the Red Sea crisis to global maritime transport: amplified carbon emissions and possible carbon pricing dysfunction*. Environmental Research Letters, Vol. 19, No. 7 (2024). https://doi.org/10.1088/1748-9326/ad59b7
- Port Economics, Management and Policy: *Routing Options between Shanghai, Rotterdam and New York*. 2024. [Online] Available at: https://porteconomicsmanagement.org/pemp/contents/part1/interoceanic-passages/routing-options-shanghai-rotterdam/ (Accessed: 10/09/2024).
- Royal Navy News: *'Unprecedented' Rise in SOS Calls from Seafarers in Red Sea Crisis*. 2024. [Online] Available at: https://www.royalnavy.mod.uk/news/2024/march/22/20240322-unprecedented-rise-in-sos-calls-from-seafarers-in-red-sea-crisis (Accessed: 04/09/2024).
- Samaan, Jean-Loup: *The Red Sea attacks highlight the erosion of US leadership in the region*. Atlantic Council, 2024. [Online] Available at: https://www.atlanticcouncil.org/blogs/menasource/red-sea-attacks-houthis-biden-administration-leadership/ (Accessed: 15/10/2024).
- Shortland, Anja – Vothknecht, Marc: *Combating "maritime terrorism" off the coast of Somalia*. European Journal of Political Economy, Vol. 27, Supplement 1 (2011), S133–S151. https://doi.org/10.1016/j.ejpoleco.2011.03.004
- Smagin, Nikita: *Russia's Outrage Over U.S. Strikes Against Houthis Is Just Bluster*. Carnegie politika, 2024. [Online] Available at: https://carnegieendowment.org/russia-eurasia/politika/2024/01/russias-outrage-over-us-strikes-against-houthis-is-just-bluster?lang=en (Accessed: 02/09/2024).
- Statista.com: *Global container freight rate index from the 12th January 2023 to the 15th August 2024*. 2024. [Online] Available at: https://www.statista.com/statistics/1440707/global-container-freight-index/ (Accessed: 03/09/2024).
- Stausbøll, Emily: *What is behind the sudden and dramatic increases in ocean freight container shipping rates?* Xeneta, 2024. [Online] Available at: https://www.xeneta.com/blog/what-is-behind-the-sudden-and-dramatic-increases-in-ocean-freight-container-shipping-rates (Accessed: 03/09/2024).
- Stewart, Phil – Ali, Idrees – Ghobari, Mohammed*: US and Britain strike Yemen in reprisal for Houthi attacks on shipping*. Reuters, 2024. [Online] Available at: https://www.reuters.com/world/us-britain-carry-out-strikes-against-houthis-yemen-officials-2024-01-11/ (Accessed: 14/08/2024).
- Symon, Damien [@detresfa_]: Damien Symon on X. Twitter, 2023. [Online] Available at: https://x.com/detresfa_/status/1735979072126423252?s=20 (Accessed: 17/09/2024).
- TASS: *Russia says US and its allies violated UNSC resolution on Red Sea*. 2024. [Online] Available at: https://tass.com/politics/1731807 (Accessed: 05/09/2024).
- Thomas-Greenfield, Linda: *Remarks in Response to Russia at a UN Security Council Briefing on the Houthi Attacks on Commercial Shipping in the Red Sea*. New York, 2024. [Online] Available at: https://usun.usmission.gov/remarks-in-response-to-russia-at-a-un-security-council-briefing-on-the-houthi-attacks-on-commercial-shipping-in-the-red-sea/ (Accessed: 25/04/2024).
- Tucker, Robert W.: *The Purposes of American Power*. Foreign Affairs, 1980. [Online] Available at: https://www.foreignaffairs.com/articles/united-states/1980-12-01/purposes-american-power (Accessed: 18/10/2024).
- U.S. Department of Defense: *Statement from Secretary of Defense Lloyd J. Austin III on Ensuring Freedom of Navigation in the Red Sea*. 2023. [Online] Available at: https://www.defense.gov/News/Releases/Release/Article/3621110/statement-from-secretary-of-defense-lloyd-j-austin-iii-on-ensuring-freedom-of-n/ (Accessed: 15/08/2024).

- Vertin, Zach: *Red Sea Rivalries: The Gulf, the Horn, and the new geopolitics of the Red Sea*. Brookings, 2019. [Online] Available at: https://www.brookings.edu/articles/red-sea-rivalries-the-gulf-the-horn-and-the-new-geopolitics-of-the-red-sea/ (Accessed: 18/10/2024).
- Vreÿ, Francois – Blaine, Mark: *Red Sea and Western Indian Ocean Attacks Expose Africa's Maritime Vulnerability*. Africa Center for Strategic Studies, 2024. [Online] Available at: https://africacenter.org/spotlight/red-sea-indian-ocean-attacks-africa-maritime-vulnerability/ (Accessed: 03/09/2024).
- Walker, Timothy: *Africa needs a stronger voice on resolving the Red Sea crisis*. Institute for Security Studies, 2024. [Online] Available at: https://issafrica.org/iss-today/africa-needs-a-stronger-voice-on-resolving-the-red-sea-crisis (Accessed: 20/08/2024).
- Yap, Wei Yim – Yang, Dong: *Geopolitical tension and shipping network disruption: Analysis of the Red Sea crisis on container port calls*. Journal of Transport Geography, Vol. 121 (104004), 2024. https://doi.org/10.1016/j.jtrangeo.2024.104004.
- Ziady, Hanna: *The shipping industry is sounding the alarm as another vessel sinks in the Red Sea*. CNN, 2024. [Online] Available at: https://edition.cnn.com/2024/06/20/business/red-sea-vessel-sunk-shipping-warning/index.html (Accessed: 07/09/2024).

HDR 2025, Nr. 1, 104–110.

Gabriella Rosta

THE ROLE FRANCE PLAYED IN THE POLITICAL LIFE OF CHAD AND OTHER FORMER AFRICAN COLONIES

DOI: 10.35926/HDR.2025.1.9

ABSTRACT: *Chad, a former French colony in the heart of the African continent, has always been a region that, until recently, seemed very remote and of little interest to the Hungarian people. However, the Hungarian government's plan for the Hungarian Defence Forces to set up a possible military mission in Chad with the participation of 200 Hungarian service members has drawn attention to the situation and events in the region. The Sahel region is today considered the most dangerous and unstable region in the world, characterised by the presence and operation of numerous terrorist organisations and frequent coups d'état, forcing millions of people every day to start a new life as refugees on the European continent, leaving their homes or perhaps their countries of origin. In this article, we review the various historical, geographical, economic, and political factors that have led to this situation, the current situation and its likely outcome, and the role and responsibility of France.*

KEYWORDS: *Africa, Chad, France, military, French Armed Forces*

ABOUT THE AUTHOR:

Gabriella Rosta is a language teacher at the Foreign Language Training Centre, Faculty of Military Sciences and Officer Training, Ludovika University of Public Service (MTMT: 35153325).

INTRODUCTION

The 4000-mile-wide area in the heart of Africa, stretching from the Atlantic to the Red Sea, is known as the Sahel Area, or the Coup Belt of Africa. Today, it is probably the most dangerous and unstable area in the world.

The area has historically been terribly deprived and plagued by poor economic governance. In recent years, however, the region has been wracked by democratic retreat, several coups d'état, high levels of terrorist violence and civil wars, and millions of its inhabitants have been forced to flee their homes or even their countries.

In the western part of the area, the populations of former French colonies are striving to establish democratic nation-states with varying degrees of success, but with real results, and have made notable progress.

In contrast, it would appear that there has been little progress in the Central African territories. Chad, the Central African Republic, Gabon, and Cameroon are all languishing under the endless rule of dictatorships backed and supported by France.[1]

[1] Tobner 2019.

The landlocked country of Chad, in the heart of the region, has always sought to be part of the chaos that surrounds it, but inside it is constantly dancing on the razor's edge. As one of the world's fastest-growing countries in terms of population, Chad's eventual direction in domestic politics will affect the fate of tens of millions of people. If the worst-case scenario is realised, the collapse of Chad, sandwiched between the Sudanese civil war in the east and the terrorist rule in the Western Sahel, could open a gateway allowing the free flow of terrorism, arms trafficking, and violence between the two chaotic regions.

The position on this side of the Atlantic Ocean has always been that Chad is a French concern. Paris's former colony continues to remain close to the colonial heartland, home to the largest French military presence on the continent, and now serves as a gathering place for the French Armed Forces retreating from other African countries. In a gesture of loyalty, France continues to confer legitimacy on successive Chadian military leaders.[2]

Since the creation of the sovereign state in 1960, there has been a continuous French military presence in Chad, which means that various groups, organisations, political formations, paramilitary, and even criminal factions have the support of France, depending on what is more in favour of the economic, political, or cultural interests of the former colonial power. We can conclude that the rule of the dictators of the last three decades could and can only be maintained by means of the French military presence and support.[3]

Numerous economic, geographical, political, and historical factors have led to this situation.

ECONOMY

In addition to strategic and political interests, France has, of course, economic ties and activities in the countries of the former colonial empire, including Chad. France has very important economic interests throughout the region: oil (Gabon, Republic of Congo, Gulf of Guinea), diamonds and uranium (Niger), cocoa and coffee (Ivory Coast), as well as banking, transport, and other services (water, communications) in both Western and Central African states.

In Francafrique, there are two types of so-called monetary unions, which allow France, even after the break-up of its colonial empire, to maintain a kind of protectorate over the countries that have gained independence. First, the CFA franc, printed by the French National Bank, is the official currency in many states of West and Central Africa, and second, member countries hold more than 50 percent of their central bank assets in the French Treasury. Africa accounts for between 0.25 and 0.5 percent of France's annual GDP growth and between nine and ten percent of French imports of raw materials.[4]

In the context of the continuing difficulties the world economy faces, it is important to maintain these links in order to preserve economic equilibrium. France needs to defend its positions against other ambitious countries seeking to penetrate the African continent, which are emerging as competitors in key areas such as finance, energy, infrastructure, telecommunications, and agriculture.[5]

[2] Powell 2021.

[3] Hudson 2023.

[4] WITS Data 2021.

[5] Sztankai 2014.

The economic prestige of French companies in the business world of former African colonies has been steadily declining over the last few decades. China, Turkey, and Morocco are gaining more and more ground in the market.

CULTURE

When we talk about France's presence in Africa, we must not forget the cultural aspect. Francophonie is the pledge of the French cultural heritage on the African continent. The teaching and use of the French language in the allied countries is essential to gain and maintain sufficient economic and political influence. It is clear that the more French-speaking countries there are, the greater the chances are of building a stronger and wider diplomatic and economic network of alliances.[6]

French is the third most widely used language in the business environment and the fourth most used in the world of the internet.

The French-speaking universe is a fast-growing market. Francophonie currently has more than 320 million speakers, representing three percent of the world's total population, and 60 percent of French speakers live in Africa. This increased by 15 percent between 2018 and 2024, and by 2050, it will account for eight percent of the world's population, with 750 million people. This huge increase is explained by the demographic growth of the African population.[7]

GEOPOLITICS

France is a middle power in terms of its role in the world economy and world politics, but also a key player on the African continent. This role justifies the fact that when the UN Security Council discusses issues affecting the region, France is always an important participant in the negotiations and also justifies its permanent presence in the international community and the UN Security Council. In order to maintain this central role, France has an essential economic and geopolitical interest in sustaining its military presence and power on the continent.[8]

HISTORY

Since the end of the colonial regime in 1960, Chad has existed in the same form: under/alongside French military occupation, which supports this or that faction according to its own interests, and helps the leaders of criminal gangs to power, who rule their people as dictators, while pursuing the aims of foreign backers. The current president, Mahamat Déby, who succeeded his father on the 'throne', and Idriss Déby, who came to power in the shadow of the sinister Hissène Habré, are both ruthless dictators who control their people through fear and violence.

These dictatorships have only survived thanks to France's military presence and support and to their success in putting down the rebellions and uprisings that have periodically sprung up to overthrow them.

[6] Sztankai 2013.

[7] Henni-Moulai 2023.

[8] Chafer 2017.

The period following the independence of the African countries that had been French colonies is known by historians as the 'Françafrique'. The difficulties of this era were faced by both the former colonial and the newly independent countries. Despite all its efforts, France's influence seems to be waning, and its presence and importance in the political and economic spheres are steadily diminishing. For the awakening social forces and the new elite, France is the perfect scapegoat for all the problems, and is making great efforts to adapt to the situation and maintain its position in the region.[9]

CHRONOLOGY OF MILITARY INTERVENTIONS

Over the last four decades, France has intervened militarily mainly on the African continent, either under intergovernmental agreements or multilateral ones.

The first operation was launched in August 1983. In the framework of Operation Manta, some 4000 French troops arrived in Chad to support the regime of Chadian President Hissène Habré, who had previously been in power, in his fight against the Libyan-backed GUNT (Goukouni Oueddei's Transitional Government of National Unity).

A few months later in the same year, the Council of Ministers approved a 1100 million French franc contribution to finance military operations in Chad.

On the first anniversary of the launch of the operation, French Defence Minister Charles Hernu, stated in a radio interview that France would continue its campaign until the Libyans left the Chadian territories they had occupied 12 years earlier.

A month later, an agreement was signed between France and Libya to withdraw from the occupied territories. At the same time, Minister of Foreign Affairs Claude Cheysson stated that Chad would continue to benefit from French military support if Libya violated the accord.

In February 1986, following Libya's breach of the agreement and the resumption of fighting between the two African countries, the French air force launched an air raid on the Ouadi Doum airfield in northern Chad, which was a base of the Libyan forces. This is known as Operation Épervier.

At the end of 1990, French Defence Minister Jean-Pierre Chevènement and Jacques Pelletier, Minister of Cooperation and Development, announced the reinforcement of the Épervier military system and support for the newly appointed Head of State, Idriss Déby, and his efforts to democratise Chad. This included the arrival of a 450-strong military contingent as a backup to help the dictator in his fight against the supporters of the former president. As a second step, a paratrooper company was sent to N'Djamena at the end of February.[10]

After that, almost a decade and a half passed without any major French military intervention. In 2006, fighter aircraft of the French air force fired warning shots against the rebels, some 250 kilometres from N'Djamena. Two years later, there was a firefight between French service members and rebels to protect N'Djamena airport and evacuate French citizens.

In January 2013, Mali requested military assistance from the French state after Islamist armed groups seized the country's capital, Bamako. This operation began under the name of Serval, commanded by the French Armed Forces, and was renamed the well-known

[9] Chafer 2002.

[10] Ministère des Armées 2025.

Barkhane a year and a half later. The operation was initially a success. French and allied ground and air forces joined to support the Malian troops. The mission was later extended to the Sahel, with two permanent bases established in Chad and Niger.

The accumulated anti-French and anti-France sentiment over the years, the unsuccessful war against the insurgents, the rise to power of the Malian junta, the escalation of violence, and the deterioration of diplomatic relations between France and Mali resulted in the decision announced by President Macron in 2022 to withdraw the French Armed Forces from Mali (Interventions de l'armée française en Afrique depuis 1981).[11]

The French Armed Forces' anti-terrorist campaign in Africa, which lasted for almost a decade, finally came to a definitive end in August 2022. In the two years since then, Operation Barkhane has been internationally and unequivocally described as a total failure, a colossal disaster of French policy.[12]

Since the military operations launched and carried out by France in the Algerian War of Independence, Chad's involvement has become the longest and most deadly foreign military engagement. It aimed to sustain the current Chadian regime to remain in power, yet it failed to prevent the fall of the bloodthirsty dictatorships of Tombalbaye (1975) and Hissène Habré (1990). It is also clearly evident that foreign military intervention in the internal affairs of another country cannot bring peace or political stability.

PRESENT SITUATION

Even after the declaration of independence of its last African colony, Djibouti, in 1977, France remained on the continent and intervened almost continuously in its internal affairs with a military presence and various actions.

Over the last two to three years, the French Armed Forces have been almost entirely squeezed out of Africa, with the number of troops stationed on the continent today (7 February 2025) reduced to just over 4000 in four bases: in Senegal (Dakar), Gabon (Libreville), Ivory Coast (Abidjan), and Djibouti.[13]

About a thousand of the French troops who were involved in Operation Barkhane and who were withdrawn from Mali, Niger, and Burkina Faso by the end of 2023 with the support of the Wagner Group, are currently stationed in Chad at three bases. In Ivory Coast, Gabon, and Senegal, the number of personnel has been reduced to 350. However, because of its strategic location, occupied by Yemen's military activity in the Bab-el-Mandeb Strait, the French base in Djibouti is not affected by the reduction. A contingent of around 1,500 troops will continue to be stationed there.

After Faya (26 December 2024) and Abeche (11 January 2025), the last French serviceman left the N'Djamena military base in Chad on 30 January 2025. This marked the end of the French army's 65-year involvement in the African country.[14]

[11] La Rédaction 2025.

[12] King 2023.

[13] Faye 2024.

[14] Molinié 2025.

PROSPECTS

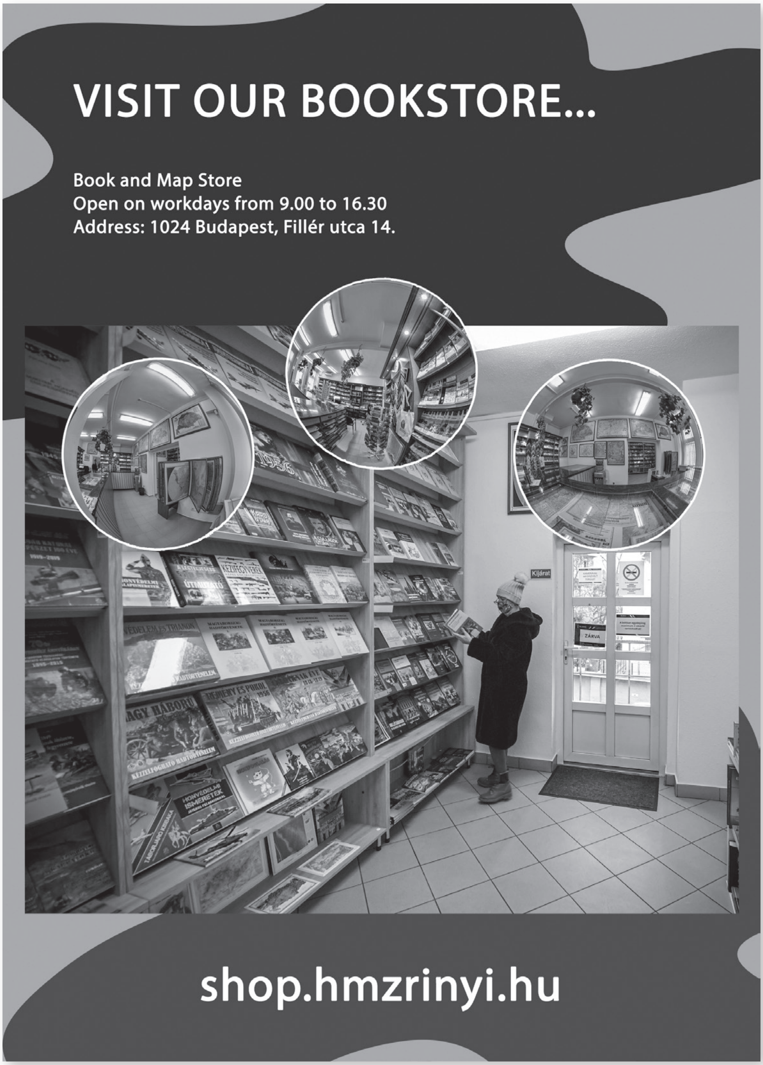
The departure of French service members coincided with the end of the UN-led MINUSMA mission in Africa, giving way to the Wagner Group to support the work of the ruling military regimes. Thousands of Wagner mercenaries are believed to already be in the region, suggesting that Russia could quickly take on a role in the power vacuum created by the withdrawal of France. Most pessimistically, Russia's military presence and the tightening economic ties with China could even lead to a proxy war. Meanwhile, the destabilisation of the region could trigger a new migration crisis in Europe.[15]

BIBLIOGRAPHY

- Chafer, Tony: *Decolonization in French West Africa*. In: *Oxford Research Encyclopaedia of African History.* Oxford University Press, Oxford, 2017.
- Chafer, Tony: *The End of Empire in French West Africa: France's Successful Decolonization?* Berg, Oxford, New York, 2002.
- Faye, Mamadou: *Les pays qui accueillent encore des bases militaires françaises en Afrique, et pourquoi*. BBC Afrique, 29 November 2024.
- Henni-Moulai, Nadia: *La francophonie en Afrique, curseur géopolitique?* TRT Français, 4 August 2023. https://www.trtfrancais.com/debats/la-francophonie-en-afrique-curseur-geopolitique-14331858 (Downloaded: 22/03/2025).
- Hudson, Cameron: *Chad: The Sahel's last domino to fall*. Center for Strategic & International Studies (CSIS), 6 December 2023. https://www.csis.org/analysis/chad-sahels-last-domino-fall (Downloaded: 22/03/2025).
- King, Isabelle: *How France Failed Mali: the End of Operation Barkhane*. Harvard International Review, 30 January 2023. https://hir.harvard.edu/how-france-failed-mali-the-end-of-operation-barkhane/ (Downloaded: 22/03/2025).
- Kolozsi, Ádám: *Putyin nyeri a legtöbbet, ha Franciaország elveszti Afrikát*. Világ, 13 August 2023.
- La Rédaction: *Interventions et présence de l'armée française en Afrique depuis 1981: chronologie*. Vie publique, République française, 7 January 2025. https://www.vie-publique.fr/eclairage/20138-chronologie-interventions-de-larmee-francaise-en-afrique-depuis-1981 (Downloaded: 22/03/2025).
- Molinié, William: *Tchad: retrait des dernières troupes françaises, ultime symbole du déclin français en Afrique*. Europe 1, Louis Epaulard (ed.), 31 January 2025.
- *Point de situation des opérations du jeudi 6 février au mercredi 12 février 2025*. Opérations, Ministère des Armées. https://www.defense.gouv.fr/operations/point-situation-operations/point-situation-operations-du-jeudi-6-fevrier-au-mercredi-12-fevrier-2025.
- Powell, Nathaniel K.: *France's Wars in Chad: Military Intervention and Decolonization in Africa*. Cambridge University Press, New York, 2021.
- Sztankai, Krisztián: *Cultural Intelligence (IC/CULTINT) – Avagy a kulturális antropológia helye és szerepe a hírszerzésben*. Hadtudományi Szemle, Vol. 6, No. 3 (2013), 131–137.

[15] Kolozsi 2023.

- Sztankai, Krisztián: *Place and Role of Cultural Anthropology in the Military.* AARMS – Academic and Applied Research in Military and Public Management Science, Vol. 13, No. 1 (2014), 113–117.
- Tobner, Odile: *Complicité de la France avec les dictateurs criminels en Afrique Centrale: Tchad, Cameroun*. Les Possibles, No. 20 (Spring 2019), 21 May 2019.
- WITS Data: *France Raw materials Imports by country and region in US$ Thousand 2021.* (Downloaded: 07/02/2025).



Aadi Rajesh

RETHINKING INDIA'S NUCLEAR DOCTRINE: CHALLENGES AND OPPORTUNITIES IN A MULTI-POLAR ASIA

DOI: 10.35926/HDR.2025.1.10

ABSTRACT: *The nuclearization of Asia's security architecture poses a significant challenge for countries across the continent and beyond. As China and India engage in a strategic competition for Asian dominance in the 21st century, the nuclear issue has become a critical policy and security challenge for both nuclear-armed rivals.*

China's explosive economic and military growth has altered the balance of power in Asia, challenging the security assumptions and architectures of countries throughout the continent. While nations remain wary of Chinese dominance, India, China's key competitor in Asia, remains focused on preventing a Chinese-dominated Asian security and economic architecture.

However, due to a shift in the balance of power in China's favour over the past three decades, India is developing strategies to reduce and mitigate the power asymmetry. Among these strategies are plans to amend its nuclear policies and explore new avenues for deterrence and offensive capabilities.

The paper will compare the nuclear doctrines of India, China, and Pakistan, examining the gaps and challenges in India's policy relative to its nuclear-armed neighbours. Additionally, it will explore how India is reimagining its nuclear policy and security strategies to counterbalance China.

KEYWORDS: *India, China, nuclear, Asian politics, security dilemma*

ABOUT THE AUTHOR:

Aadi Rajesh is a PhD student at the Ludovika University of Public Service Doctoral School of Public Administration Sciences, specializing in international relations and security studies (ORCID: 0009-0002-9345-5073; MTMT: 10097622).

METHODOLOGY

The study focuses on hard power strategies for a military strength analysis between India and China. It also examines the economic, industrial, and technological capabilities of both countries, as well as the power dynamics and relations between the two Asian powers. The study also includes Pakistan, which is itself a nuclear power and augments Chinese power with its formal military alliance. This paper focuses on the nuclear question and nuclear security, analysing them from the perspective of power disparities, rather than exploring diplomatic negotiations or soft power dynamics.

INTRODUCTION

Since the fall of the Soviet Union in the 1990s, the continental politics of Asia have been in a constant flux, with China and India competing for Asian primacy as part of their long-term ambitions. While having similar-sized economies in the 1990s, China has leapfrogged India and become a comparatively stronger economic and industrial power, which has given its military a financial, technological, and strategic advantage over India.[1]

China, as of 2025, is an 18 trillion USD economy, which is more than four times larger than India's.[2] Furthermore, China's defence budget is over 230 billion USD, compared to the 72 billion of India,[3] which has given the former the ability to create one of the largest defence industrial and manufacturing bases in the world and strong investments in modern technologies such as artificial intelligence, 5th generation fighter aircraft, aircraft carriers, cybersecurity capabilities, etc.

In response to the growing gap compared to China and the challenges it presents, India has adopted multiple diplomatic strategies, including partnerships with countries like Vietnam and the Philippines, and participation in the Quad[4] alongside Japan, Australia, and the United States. Nonetheless, these efforts have not fully succeeded in curbing Chinese ambitions, as evidenced by the ongoing border tensions, such as the 2022 Yangtse clash and the 2020 Galwan Valley incident, where 20 Indian and at least 4 Chinese soldiers were killed.[5]

This power imbalance between India and China and India's inability to diplomatically counter and contain China has opened arguments among Indian strategic and defence experts on altering India's highly restrictive, no-first-use nuclear doctrine and exploring and expanding options of first strike and pre-emptive strike capabilities.

INDIA'S NUCLEAR DOCTRINE

India as a nation was born following the ideals of Mahatma Gandhi and his ideas of ahimsa, i.e., nonviolence. However, due to the 1962 war with China and various threats from the Western and Eastern worlds, the country decided to go nuclear,[6] and in 1974, it did its first nuclear test, followed by a second, successful one in 1999.

Following the 1999 nuclear tests, India released its Draft Nuclear Doctrine (DND) in August 1999 and its first full nuclear policy in January 2003.[7]

India's nuclear doctrine is based on three major principles: the no-first-use policy, which commits India to not using nuclear weapons pre-emptively; maintaining credible deterrence, where India ensures a small but effective nuclear arsenal; and non-proliferation, where India supports global nuclear disarmament while maintaining strict control over nuclear materials and technology.[8]

[1] Tellis – Mirski 2013.

[2] Galani 2024.

[3] Security Risks Research 2024.

[4] Quadrilateral Security Dialogue.

[5] Rajeev – Stephenson 2023.

[6] Jha 1998.

[7] Rajagopalan 2016.

[8] Prime Minister's Office 2003.

India's no-first-use policy is an example of deterrence and defensive strategies, and means that India is strongly committed to not using nuclear weapons first in any conflict. In the policy, India maintains that it will only use nuclear weapons in retaliation if attacked with nuclear weapons by any other party. Furthermore, the Indian policy states that upon being attacked with nuclear weapons, India's response will be massive retaliation.[9]

India's credible minimum deterrence means that it will only maintain the least number of nuclear warheads needed to deter its nuclear rivals. Under this policy, India has not attempted to gain superiority in numbers over either Pakistan or China and will maintain the minimum number of warheads needed for credible deterrence (see Figure 1).[10]

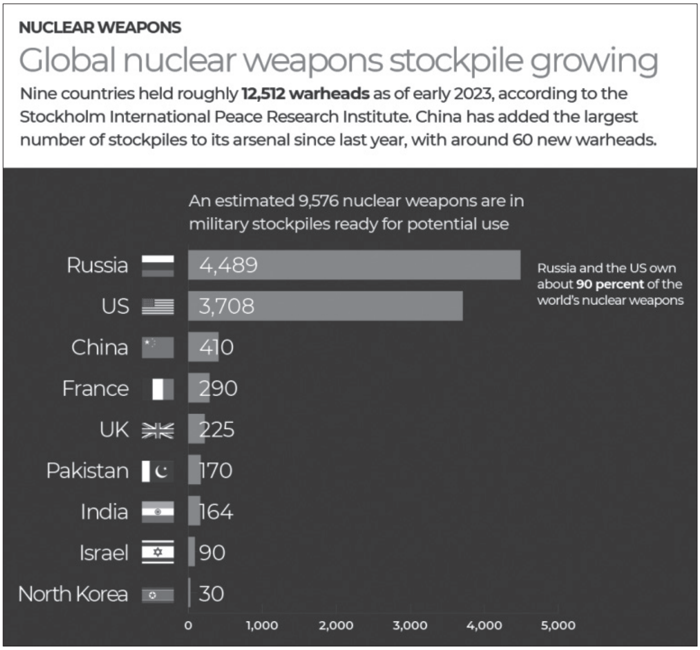


Figure 1 *Global nuclear weapons stockpile growing*

Source: *https://www.aljazeera.com/news/2023/6/12/china-other-states-fortify-nuclear-weapons-arsenals-report*

India's principle of non-proliferation means that the country remains deeply committed to strict civilian and political control of nuclear weapons, primarily through the Nuclear Command Authority (NCA). Furthermore, even though India is not a signatory to the Nuclear Non-Proliferation Treaty (NPT) and the Comprehensive Nuclear-Test-Ban Treaty (CTBT), it follows the norms of these treaties and is strongly committed to preventing the spread of nuclear weapons and technologies.[11]

[9] Rajagopalan 2009.
[10] Rajagopalan 2009.
[11] Rajagopalan 2009.

Another aspect of India's policy is the Cold Start Doctrine. Although the Cold Start Doctrine is not part of the nuclear policy, it is part of the conventional military strategy and is directly related to the use of nuclear weapons in war.[12]

According to the Cold Start Doctrine, to counter Pakistan's first-strike-capable nuclear doctrine, special integrated battle groups (IBGs) would swiftly enter the territory of Pakistan and seek control over the country's nuclear weapons to avoid and prevent a nuclear war.

These policies have evolved from India's core ethos of non-violence and the belief in dialogue and diplomacy to resolve contested issues. This strategic thinking has been the cornerstone of Indian foreign and military policy, but considering the growing strength of China and its alliance with Pakistan, China's growing nuclear arsenal and assertiveness, and Pakistan's more aggressive pre-emptive nuclear use policies, India has begun to rethink and reanalyse its own nuclear policy.

CHINA'S AND PAKISTAN'S NUCLEAR DOCTRINES

China's nuclear policy remains to create a strong, credible nuclear deterrence against its two main rivals, India and the United States.

Similar to that of India, China maintains a no-first-use policy and deterrence as its nuclear policy.[13] However, compared to India, China's policy on the ground is much more effective due to its more advanced nuclear capabilities and technologies. China possesses more than 400 nuclear weapons, significantly surpassing India's arsenal of 160, and has established a robust second-strike capability.[14]

Moreover, due to its vast financial resources and industrial capacity, China is rapidly modernising its equipment and investing in new technologies. Furthermore, China's nuclear triad, which includes land, air, and sea-based launch platforms, is more advanced than India's nuclear triad.[15]

The rapid strengthening of China's nuclear arsenal and technology has significantly enhanced its nuclear capabilities, giving it an advantage over India in the nuclear competition. Furthermore, China's military alliance with Pakistan has bolstered its strength and created a power imbalance in Asia.

Pakistan's nuclear capabilities, although weaker than India's, compensate for its technological and financial limitations through a more aggressive nuclear policy. Unlike India and China, which have committed to a no-first-use policy, Pakistan's nuclear doctrine maintains the option for the first use of nuclear weapons.[16]

Pakistan reserves the option to use nuclear weapons in conventional wars, particularly in the event of a strategic defeat or existential threat. This first-use policy is designed to counter India's significant economic and military superiority, as well as its technological capabilities.[17]

[12] Ladwig 2007/08.

[13] Pande 2000.

[14] Kurita 2018.

[15] Kurita 2018.

[16] Center for Arms Control and Non-Proliferation 2023.

[17] Center for Arms Control and Non-Proliferation 2023.

Pakistan has also invested heavily in smaller, tactical nuclear weapons, such as the Nasr missile, to challenge India's Cold Start Doctrine.[18] These tactical nuclear weapons (TNWs) are part of Pakistan's Full-Spectrum Deterrence (FSD) strategy, which involves developing low-yield nuclear weapons for battlefield use, rather than strategic long-range deterrence.[19]

Also, while India's or China's nuclear weapons can only be used by top leaders, as second-strike options, Pakistan's low-yield nuclear weapons can be used by a larger group of commanders and leaders in case of war with India, which increases the risk of miscalculation, unauthorized use, and vulnerability to theft due to their smaller size.[20]

Hence, due to China's strategic, technological, and tactical superiority in terms of nuclear weapons and overall military capabilities over India and Pakistan's aggressive first-use policy of tactical nuclear weapons, India is reimagining its own nuclear policy as part of a more comprehensive and long-term military and security policy.[21]

REIMAGINING INDIA'S NUCLEAR DOCTRINE

Since the victory of Prime Minister Narendra Modi in the parliamentary elections of 2014, India's ruling party has promised to revisit and revise India's nuclear doctrine. The debates on reimagining India's nuclear doctrine have split experts into two main groups: the moderates and the expansionists.[22] While moderates in the Indian strategic circles argue in favour of India's no-first-strike policy, expansionists focus on changing the policy to reflect modern realities and safeguard India's interests.

Moderates, who are status-quo supporters, firmly believe that India's nuclear policy is adequate and remains highly effective in balancing China and Pakistan. They argue that changing India's nuclear policy would harm the country's image of being a responsible nuclear power and would damage its reputation as a trustworthy partner. Furthermore, they argue that making India's policy more aggressive would lower the overall nuclear threshold and make nuclear war more likely.[23]

Expansionists, or the doctrine revisionists, believe that India's nuclear doctrine should be improved to match modern reality, especially to respond to Pakistan's first-strike-capable nuclear policy. Expansionists argue that making the nuclear policy more aggressive would increase deterrence and reduce the chances of a nuclear war in Asia.[24]

While both moderates and expansionists have found traction in Indian strategic circles, changes in India's nuclear policy remain highly unlikely in the near future. Instead, India remains committed to narrowing the gap with China by investing heavily in its second-strike capabilities and building a more robust nuclear arsenal.[25]

[18] Ahmed 2016.
[19] Bommakanti 2023.
[20] Sankaran 2015.
[21] Rajagopalan 2016.
[22] Rajagopalan 2016.
[23] Rajagopalan 2016.
[24] Rajagopalan 2016.
[25] Rajagopalan 2016.

Analysts argue that one ambiguous aspect of India's nuclear doctrine is the provision for massive retaliation in the event of a nuclear attack on India.[26] They claim that this approach would not only be financially burdensome but also potentially catastrophic for human civilization, given the risk of nuclear winter. Several experts advocate for developing more flexible deterrence strategies, such as creating tactical nuclear weapons, akin to those of Pakistan. This would enable India to employ low-yield weapons, targeting critical enemy targets and offering an alternative to its current massive retaliation policy.

Despite India's stated nuclear policy, the aspect of no-first strike remains ambiguous. In a 2010 speech, Indian national security advisor Shivshankar Menon stated that India's no-first-use policy applies only to non-nuclear states,[27] leading some analysts to argue that this policy may not apply to nuclear-armed states like China and Pakistan.

Moreover, the use of biological, chemical, and emerging weapons, capable of causing significant harm to a nation, remains vague for both nuclear and non-nuclear states.[28]

Beyond nuclear reform options and enhancing its defence technological and manufacturing capabilities, analysts and experts argue in favour of strengthening India's strategic partnerships with Southeast Asian countries such as Indonesia, Vietnam, and the Philippines to counter the China–Pakistan alliance. The Philippines has already acquired supersonic BrahMos missiles from India, and while India adheres to strict nuclear controls, it could arm Southeast Asian nations with conventional weapons to reduce the strategic and tactical military gap with China.[29]

Analysts debating the reform of India's nuclear policy also discuss the consequences of such changes. They argue about various direct and indirect consequences that could arise from altering the nuclear policy of the country.

While Pakistan maintains a policy of using nuclear weapons first, even in conventional wars, both India and China have consistently adhered to a no-first-use policy. If India were to change its policy, China might alter its own nuclear doctrine to counter the Indian threat, potentially increasing the risk of nuclear conflict in Asia.

Furthermore, beyond India, China, and Pakistan, Israel and North Korea also possess nuclear weapons, and Iran is making significant investments in nuclear technology. An update to India's nuclear policy could set a precedent for these nations, potentially destabilizing not only Asian continental politics but also putting the future of human civilization at risk.

GEO-POLITICAL IMPLICATIONS

While India shares a strong relationship with the US, Russia, and various other global and regional powers, the upgradation of its nuclear policy could trigger diplomatic challenges and possible sanctions from various nations.

India, which is progressing economically, might face economic hardships in case of economic sanctions, and if threatened, smaller south Asian states, such as Nepal or Sri Lanka, could join Pakistan in a formal military alliance with China, which could not only isolate India in South Asia, but also create security challenges in its traditional sphere of influence.

[26] Dupar 2017.

[27] Sundaram – Ramana 2018.

[28] Sundaram – Ramana 2018.

[29] Kumar 2025.

The United States would also face challenges in accepting India's aggressive nuclear strategies, as it could set a precedent for Iran and North Korea to use the Indian example to justify their own nuclear procurements and expansion.

Furthermore, countries like Germany and Japan, which are strong economic partners of India, could be forced to impose sanctions on India due to the strong anti-nuclear lobby groups in those countries, respectively.

CONCLUSION

While India's ideas of non-violence and its no-first-strike nuclear doctrine have been integral parts of Indian strategic thinking, the changing global power dynamics and the rise of its key rival, China, call into question the validity of India's policy.

China, being a larger economy and a permanent veto member of the UN Security Council, with its declared aim of Asian primacy, has questioned the security and economic order in Asia, challenging its key Asian rival, India.

As the balance of power tilts in China's favour and its alliance with Pakistan deepens, Indian analysts are urging a re-evaluation and adoption of new nuclear policies that reflect contemporary realities and effectively address the mounting nuclear challenges presented by the China–Pakistan axis.

India could mitigate the challenges posed by China and Pakistan by reimagining its nuclear strategy, investing in newer technologies and deterrence mechanisms, and establishing key alliances in Asia. Nonetheless, challenges will remain due to the risk of a more aggressive Chinese retaliation policy and the lowering of the nuclear war threshold in Asia.

As a responsible nuclear power, India must bridge the gaps in its technological, economic, and strategic capabilities relative to China to create a stable, long-term Asian political, security, and economic order.

BIBLIOGRAPHY

- Ahmed, Mansoor: *Pakistan's Tactical Nuclear Weapons and Their Impact on Stability*. Carnegie Endowment for International Peace, 30 June 2016. https://carnegieendowment.org/research/2016/06/pakistans-tactical-nuclear-weapons-and-their-impact-on-stability?lang=en
- Bommakanti, Kartik: *Pakistan's latest nuclear antics in the form of Full Spectrum Deterrence*. Observer Research Foundation, 4 July 2023. https://www.orfonline.org/expert-speak/pakistans-latest-nuclear-antics-in-the-form-of-full-spectrum-deterrence
- Center for Arms Control and Non-Proliferation: *India and Pakistan – Center for Arms Control and Non-Proliferation*. 12 July 2023. https://armscontrolcenter.org/countries/india-and-pakistan/
- Dupar, Mairi (ed.): *Credibility of India's massive retaliation*. Observer Research Foundation, 9 January 2017. https://www.orfonline.org/research/credibility-indias-massive-retaliation
- Galani, Una: *India starts resembling China in unflattering ways*. Reuters, 19 December 2024. https://www.reuters.com/breakingviews/india-starts-resembling-china-unflattering-ways-2024-12-19/
- International Campaign to Abolish Nuclear Weapons (ICAN): *Which countries have nuclear weapons?* [no year]. https://www.icanw.org/nuclear_arsenals
- Jha, Prem Shankar: *Why India Went Nuclear*. World Affairs: The Journal of International Issues, Vol. 2, No. 3 (1998), 80–96. http://www.jstor.org/stable/45064543

- Kumar, Atul: *Shaping China's periphery: BrahMos missiles in Southeast Asia*. Observer Research Foundation, 21 January 2025. https://www.orfonline.org/expert-speak/shaping-china-s-periphery-brahmos-missiles-in-southeast-asia
- Kurita, Masahiro: *China-India Relationship and Nuclear Deterrence*. In: NIDS Journal of Defense and Security, 19 December 2018, 37–61. https://www.nids.mod.go.jp/english/publication/kiyo/pdf/2018/bulletin_e2018_4.pdf
- Ladwig III, Walter: *A cold start for hot wars? The Indian Army's new limited war doctrine*. Belfer Center for Science and International Affairs, Winter 2007/08. https://www.belfercenter.org/publication/cold-start-hot-wars-indian-armys-new-limited-war-doctrine
- Pande, Savita: *Chinese Nuclear Doctrine*. Strategic Analysis: A Monthly Journal of the IDSA, Vol. XXIII, No. 12 (2000). https://ciaotest.cc.columbia.edu/olj/sa/sa_00pas01.html
- Prime Minister's Office: *Cabinet Committee on Security Reviews Progress in Operationalizing India's Nuclear Doctrine*. Press Information Bureau (PIB) press release, 4 January 2003. https://archive.pib.gov.in/archive/releases98/lyr2003/rjan2003/04012003/r040120033.html
- Rajagopalan, Rajesh: *India's Nuclear Policy*. 2009.
- Rajagopalan, Rajesh: *India's Nuclear Doctrine Debate*. Carnegie Endowment for International Peace, 30 June 2016. https://carnegieendowment.org/research/2016/06/indias-nuclear-doctrine-debate?lang=en
- Rajeev, Nishant – Stephenson, Alex: *Why We Should All Worry about the China-India Border Dispute*. United States Institute for Peace, 2023. https://www.usip.org/publications/2023/05/why-we-should-all-worry-about-china-india-border-dispute
- Sankaran, Jaganath: *Pakistan's Battlefield Nuclear Policy: A Risky Solution to an Exaggerated Threat*. International Security, Vol. 39, No. 3 (2015), 118–151. https://doi.org/10.1162/isec_a_00191
- Security Risks Research: *Comparison India China Defence Budget 2024–25*. 8 March 2024. https://www.security-risks.com/post/comparison-india-china-defence-budget-2024-25
- Sundaram, Kumar – Ramana, M. V.: *India and the Policy of No First Use of Nuclear Weapons*. Journal for Peace and Nuclear Disarmament, Vol. 1, No. 1 (2018), 152–168. https://doi.org/10.1080/25751654.2018.1438737
- Tellis, Ashley J. – Mirski, Sean: *Crux of Asia: China, India, and the Emerging Global Order*. Carnegie Endowment for International Peace, 10 January 2013. https://carnegieendowment.org/research/2013/01/crux-of-asia-china-india-and-the-emerging-global-order?lang=en

EDITORIAL POLICIES

PEER REVIEW PROCESS

In order to ensure that articles are of a high quality, all submissions are reviewed by at least two subject matter experts. The review process is anonymous and confidential (double-blind peer review).

OPEN ACCESS POLICY

The General Staff of the Hungarian Defence Force grants permission to institutions of higher learning to deposit in their repositories scholarly articles authored or co-authored by their researchers and published in *Hungarian Defence Review,* provided that the final publisher's version is archived and its layout is kept intact, and

a. The link to the original publication is provided;
b. The publication details are included as part of the metadata;
c. The publisher *(Hungarian Defence Review)* is indicated.

Articles published in *Hungarian Defence Review* may also be reproduced electronically or in print as instruction materials in professional courses for military and civilian specialists, provided that full bibliographic information and a link to the original publication are provided to the readers. The Editors request that they be informed when material published in the journal is used as instruction material.

The authors of articles published in *Hungarian Defence Review* are authorized to make their work accessible to the public through their websites, provided the above conditions are met.

ETHICAL GUIDELINES

Hungarian Defence Review is committed to the dissemination of high-quality research through its articles according to the set norms and ethics of the social scientific community. Conformance with the standards of ethical behaviour and norms of research of all involved in the process, namely the editors, the editorial advisory board, peer reviewers, publisher(s), and contributors to the publication is important in order to maintain a cutting-edge journal worthy of international academic citizenship. In particular, the following is required of the stakeholders:

Editorial Advisory Board – The Editorial Advisory Board consists of recognised and well-known academics, theorists and expert practitioners in their subject area. The Editorial Advisory Board members act as an example and subscribe to the norms and ethical standards of the international scientific community and the ethical guidelines of this journal. While the members' task is mainly advisory in nature, they also provide advice and serve as a source of experience during the review and publication process as set out in the instructions to authors and the particular ethical guidelines for the journal set out here.

Editors – Editors evaluate manuscripts only in terms of their academic merit and suitability in terms of the focus of the journal. Editors take care that the selected peer reviewers are academics in good standing and with suitable knowledge and expertise in the particular field of the article submitted. Editors will take responsible and reasonable responsive measures with regard to ethical complaints received. Complaints of ethical transgressions will be investigated and reasonable steps taken as per the circumstances of a particular case.

Authors – Authors should ensure that their submissions are their own original work, sufficient in detail, well-argued, and according to a proper reference system (consult the *Hungarian Defence Review* guidelines for authors). Where the works of other authors are used proper and full referencing is required. No paraphrasing or indirect paraphrasing is acceptable without attribution. All sources will be properly acknowledged. Plagiarism in any of its forms, whether construed as unconscious or naïve plagiarism, direct or indirect plagiarism, is unacceptable and will lead to immediate rejection of articles including the blacklisting of the person involved. Submitting an article or review article to more than one journal is not acceptable. Where co-authorship is at stake the person responsible for submission will ensure that the co-author(s) concur on the submission in that particular version both in terms of contents, argument, and format.

Reviewers – *Hungarian Defence Review* uses a double-blind peer-review process. All articles/submissions are treated as strictly confidential. All information obtained through the peer-review process, including research data, is not for use by the reviewers or anyone associated with the reviewer either privately or for purposes of dissemination. Peer reviewers strive to conduct their reviews in an unbiased way and observations and comments (including constructive criticism or the identification of shortcomings in articles) are to be formulated clearly and with supporting arguments. Any peer reviewer that feels unqualified or not interested for any reason in reviewing a particular submission should notify the editors and kindly excuse himself from the process. Reviewers should under no circumstances review articles in which they observe and/or are aware of a conflict of interests, be it due to personal, collaborative, or competitive relationships, connections or networks during the process from the start of the initial article to the publication of the output. Reviewers should respond according to the set requirements and feedback period in good time as requested by the editors to the benefit of the authors and the journal.

GUIDELINES FOR AUTHORS

CONDITIONS FOR PUBLICATION IN THE HUNGARIAN DEFENCE REVIEW

The Hungarian Defence Review is the English language special edition of Honvédségi Szemle, the flagship professional journal of the Hungarian Defence Forces. It provides an opportunity to publish papers on subjects that match the various sections. The maximum length of papers is 40,000 characters, including notes and the captions of figures and tables. The submissions are subject to double-blind peer review. The Editorial Board reserves the right to apply such corrections to the grammar, composition, and style of submissions as will not change the author's original intent.

The Editorial Board issues a certificate of acceptance only if the Editorial Board – relying on the reviewers' recommendation – decides in favour of publishing the submission. After the acceptance of the paper, the journal's publisher, HM Zrínyi Nonprofit Kft., signs a contract with the author, which regulates issues related to publication and copyright. In order to allow an orderly editorial process – and to comply with the requirements set by the Hungarian Academy of Sciences – the authors are requested to comply with the following:

- Send the manuscript as an attachment to electronic mail (in Microsoft Word .doc or .docx format) to the Editorial Office (hdr@hmzrinyi.hu).
- At the beginning of the document state your name, rank, position (occupation), institution, academic degree and contact details (e-mail address, phone number). If you want your paper to be included in the Hungarian depository of scientific papers, provide your ORCID number, as well as the MTMT code, if any. This information is absolutely necessary in order for the work to be included in the Hungarian MTMT and the Real Repository in electronic form.
- Place a one-paragraph abstract (approx. 800-1,110 characters), as well as three to five keywords at the beginning of the text. The abstract should be written in the third person, i.e., without personal references, and it should not duplicate the introduction in the main text.
- In order to clarify the level of the various chapters and subchapters, their titles should be supplemented by parenthetical codes (K1, K2, K3) corresponding to the appropriate level. There should be no more than three levels.
- If figures (maps, graphs, drawings) or tables are used to illustrate the narrative, these should be in English. If this is not possible, the translated graphic text should be included. The journal is printed in black-and-white and grayscale. The figures should be prepared accordingly, preferably as simple, line drawings with legible captions. The illustrations should also be submitted as separate attachments, in editable (jpg, tiff) format, with a resolution of 300 dpi, min. 2000 pixels wide. Figures and tables should be numbered, with captions that, in addition to the title of the figure or table, indicates its author or source, and the date of download if it was downloaded from internet.
- Photo illustrations are accepted only in particularly justified cases. In this case, also make sure that the resolution is of the right size (300 dpi) and indicate the source of the image as in the case of figures.

– With the exception of the Forum and Review sections, the journal publishes only original, unpublished works prepared in accordance with scientific standards, with the cited source iterature referenced and listed appropriately.
– The editors assign DOI identifier to the papers and upload them to the MTMT after their publication. Please do not upload your paper yourself, as this may lead to disruptions. If, for some reason, it is urgent that the paper be uploaded, please let the editors know.

STYLE AND FORMATTING

Use 12-point Times New Roman font in the body of the manuscript, and 10-point Times New Roman in the footnotes.

Use 1.5 line spacing, and 8-point spacing after each pararaph instead of indenting the first line.

The preferred spelling is UK English, however, other spelling is also accepted, as long as it is consistent throughout the text. However, when quoting a source exactly, use the spelling in the original text. Dates may be written with numbers, in the order appropriate for the regional English spelling the author selected (UK, USA, Indian, etc., e.g. 03.01.2014). However, in order to avoid confusion, it is preferable to spell out the month, or use its three-letter abbreviation. Words and expressions not commonly used outside a particular region or country should be explained in parenthesis or in a footnote.

Use double qutation marks ("…") when quoting a source exactly. Use single quotation marks ('…') for a quotation within a quotation. Long quotations are discouraged. To shorten quotations, omit unnecessary words and phrases. Use ellipsis (…) to indicate places where text was omitted. When the quoted text is longer than two lines in the manuscript, it should be italicised, formatted as a separate paragraph, and given wider margins than the body of the text.

Spell out whole numbers under 11. For numbers longer than three digits, use a comma to separate the thousands, millions, etc.: 1,000, 100,000, etc. Do not use the Indian numbering system of laks and crores. Use a perid to indicate decimals: 0.2, 123.21, etc. When a number identifies a military unit, the particular model of a vehicle or other equipmpent, a city district, etc., use the original format: XVIII Airborne Corps, 82nd Airborne division, 2^{e} REP, M777 howitzer.

The first in-text reference to an abbreviation must be written out in parentheses. If the abbreviation is that of a phrase in a language other than English, then provide the translation in parentheses as well: MPLA (Movimento Popular de Libertação de Angola – People's Movement for the Liberation of Angola).

Subdivide the manuscript into logical units, and give each section a short title. Do not go overboard with the subdivisions: more than two levels of subdivision is discouraged.

Bulleted lists are acceptable, where appropriate.

FOOTNOTES

References to the source literature should be made on the page where the work is cited, without typographic highlights (for example, italics), as a footnote (and not as an endnote), indicating the page number (if necessary).

If more than one source work must be cited at a given point in the text, only one superscript number should be used, and the works should be included in a single footnote, separated by semicolons.

Explanatory and additional information should also be placed in the footnotes.

LITERATURE USED

Place the list of the source literature at the end of the paper in alphabetical order, in accordance with the first letter of the author's last name. If a source also has a DOI identifier, please indicate it after entering the bibliographic data. Include only such works in the list as are referenced in the main text and are listed in the footnotes. Do not include sources that were consulted, but are not quoted in the manuscript.

If a referenced source was published in a language that uses a non-Latin script (Arabic, Russian, etc.), the author must transcribe all bibliographic data in the reference into Latin script.

It is recommended (although not mandatory) to provide a translation in parentheses of the titles of referenced works written in languages other than English.

Reference formatting requirements			
type of work cited	**content of citation**	**in bibliography**	**in footnote**
		In the Bibliography, page numbers are indicated only for collections and journals (i.e., chapter or article). In terms of formatting, only the title is italicized; do not use underlining, bold, or lowercase letters.	No page numbers are necessary if reference is made to the entire work. For a specific quote, indicate the page number or page range. Do not use any formatting (italics, underlining, bold, small capital letters).

Reference formatting requirements			
type of work cited	**content of citation**	**in bibliography**	**in footnote**
Work by a single author	Surname, First name: *Title*. Publisher, place of publication, year of publication.	Abdullah, Sheikh Mohammad: *Flames of the Chinar: An Autobiography.* Penguin Books India, New Delhi, 1993. Bellavia, David: *House to House: An Epic Memoir of War.* Pocket Star, New York, 2008.	Abdullah 1993. Bellavia 2008, 34–36.
Work by two authors	Surname, First name 1 – Surname, First name 2: *Title*. Publisher, place of publication, year of publication.	Cederberg, Aapo – Eronen, Pasi: *How can Societies be Defended against Hybrid Threats?* Geneva Centre for Security Policy, Geneva, 2015. Detraz, Nicole – Betsill, Michele M.: *Climate Change and Environment Security: For Whom the Discourse Shifts.* International Studies Perspectives, International Studies Association, 2009.	Cederberg – Eronen 2015. Detraz – Betsill 2009, 303–320.
Work by three or more authors	Surname, First name 1 – Surname, First name 2 – Surname, First name 3 – etc.: *Title*. Publisher, place of publication, year of publication.	Hill, Napoleon – Verma, Satish – Green, Don: *Adversity & Advantage: Achieving Success in the Face of Challenges.* Union Square & Co., New York, 2021.	Hill et al. 2021, 15.
Collection of papers (entire volume)	Surname, First name (ed.): *Title*. Publisher, place of publication, year of publication.	Graham, Hugh Davis – Gurr, Ted Robert (eds.): *The History of Violence in America: A Report to the National Commission on the Causes and Prevention of Violence.* Bantam Books, New York, 1969. Shaffer, Ryan (ed.): *The Handbook of African Intelligence Cultures.* Rowman and Littlefield, 2023.	Graham – Gurr (eds.) 1969, 55. Shaffer (ed.) 2023, 731–746.
Collection of papers (one paper cited), or book chapter	Surname, First name: *Title of paper or chapter.* In: Editor name (ed.): Book title. Publisher, place of publication, year of publication, page number range.	Kiss, Peter A.: *The Bear, the Eagle and the Elephant: The Counterinsurgency Doctrines of Russia, the United States and India.* In: Sahni, Ajay (ed.): The Fragility of Order: Essays in Honour of K.P.S. Gill, Kautilya Books, New Delhi, 2019, 21–38. Santy, Patricia A.: *Behavior and performance in the space environment.* In: Churchill, S. (ed.): Fundamentals of Space Life Sciences. Krieger Publishing Company, Malabar, Florida, 1997, 45–81.	Kiss 2019, 21–38. Santy 1997, 45–81.

Reference formatting requirements			
type of work cited	content of citation	in bibliography	in footnote
Journal article (printed)	Surname, First name: *Title of the paper.* Journal title, Volume, year/ number, page number range.	Talbot, Ian: *Partition of India: The Human Dimension*. Cultural and Social History, Volume 6, 2009 – Issue 4, pp. 403–410. The volume is shown with the same type of characters as the original (i.e. with the Arabic or Roman numerals as in the imprint or on the cover).	Talbot 2009, 403–410.
Journal article (electronic)	Surname, First name: *Title of the paper.* Title of periodical, year/ number, page number range. URL or DOI (Date of Download).	Halem, Harry: *Ukraine's Lessons for Future Combat: Unmanned Aerial Systems and Deep Strike*. Parameters, Vol. 53, No. 4 (2023), 21–34. https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=3257&context=parameters (Downloaded: 02/05/2024). Kundnani, Hans: *Germany as a Geo-economic Power.* The Washington Quarterly, Vol. XXXIV. 2011/3., 40–42. researchgate.net/publication/233448698_Germany_as_a_Geo-economic_Power (Downloaded: 09/04/2018).	Halem 2023, 21–34. Kundnani 2011, 40–42.
Dissertation, term paper, manuscript, etc.	Surname, First name: *Title.* Nature of work, Institution, year.	Fabian, Sandor: *Professional Irregular Defense Forces: the other Side of COIN*. Master's Thesis, Naval Postgraduate School, 2012.	Fabian 2012, 10.
Electronic book	Surname, First name: *Title.* Publisher, place of publication, year of publication. URL (Date of Download).	Brown, William A.: *The Gilgit Rebellion 1947.* [PDF] Ibex, London, 1998. http://pahar.in/pahar/1998-the-gilgit-rebellion-1947-by-brown-s-pdf/ (Downloaded: 02/04/2024). If the e-book is not available free of charge or at a public address, please indicate the wider source of purchase (e.g. amazon.com) if possible. If the source does not contain page numbers, the chapter, and public address, identify the place based on the paragraph, e.g., Chapter 1, paragraph 3. This should be indicated after the publication year, in the same place where the page range is used. If the material does not contain chapters, headings, or markings suitable for identifying the place, then the first few words of the part in question are quoted in quotation marks, e.g., "The question of profitability…"	Brown 1998, 44.
Blog entry	Surname, First name: *The title of the post.* Website address, publication date. URL (Date of Download).	Jenkins, Brian Michael: *Consequences of the War in Ukraine: The Economic Fallout.* TheRANDBlog, 03/27/2023. https://www.rand.org/pubs/commentary/2023/03/consequences-of-the-war-in-ukraine-the-economic-fallout.html (Downloaded: 02/04/2024).	Jenkins 2024.

Reference formatting requirements			
type of work cited	**content of citation**	**in bibliography**	**in footnote**
Internet content (general, not articles, not posts)	Author (if any): *Title*. Date (if applicable). URL (Date of Download).	Lincoln, Abraham: *The Gettysburg Address*. 11/19/1863. https://www.abrahamlincolnonline.org/lincoln/speeches/gettysburg.htm (Downloaded: 02/04/2024). *United States Declaration of Independence*. 1776. https://www.archives.gov/founding-docs/declaration-transcript (Downloaded: 02/04/2024).	Lincoln, 1863. US Declaration of Independence, 1776.
One author with several works from various years, within one footnote		Schmid, Johann: *Die Dialektik Von Angriff Und Verteidigung. Clausewitz und die stärkere Form des Kriegführens*. VS Verlag, Wiesbaden, 2011. Schmid, Johann: *Hybrid warfare on the Ukrainian battlefield: developing theory based on empirical evidence*. Journal on Baltic Security 5 (1): 5–15. 2019. In short references, the surname is not repeated, only the years of publication are placed next to each other, separated by semicolons.	Schmid 2011, 15.; 2019, 5–15.
One author with several works from the same year, within one footnote	Surname, First name: *Title*. Publisher, place of publication, year of publication [a, b, c…].	Lamb, Alastair: *The McMahon Line: A Study in the Relations between India, China and Tibet, 1904 to 1914. Volume I: Morley, Minto and Non-Interference in Tibet*. Routledge & Kegan Paul, London, 1966. Lamb, Alastair: *Crisis in Kashmir 1947 to 1966*. Routledge & Kegan Paul, London, 1966.	Lamb 1966a, 20. Lamb 1966b, 42.
Authors with the same last name, same publication year, within one footnote	Surname, First name: *Title*. Publisher, place of publication, year of publication.	Verma, Kunal: *1965: A Western Sunrise: India's War with Pakistan*. Aleph Book Company, New Delhi, 2021. Verma, Aparna: *The Boy with Fire*. New Degree Press, Potomac, 2021.	Verma, K. 2021. Verma, A. 2021. Initials of the first names. If those are identical, provide the full first name.
Authors with the same last name, different year of publication	Surname, First name: *Title*. Publisher, place of publication, year of publication.	Brown, Percy: *Picturesque Nepal*. Adam and Charles Black, London, 1912. Brown, William A.: *The Gilgit Rebellion 1947*. Ibex, London, 1998.	Brown, 1912. Brown, 1998. The year alone distinguishes the authors.

Reference formatting requirements			
type of work cited	**content of citation**	**in bibliography**	**in footnote**
Indicating original publication date (for facsimile or reprint edition)	Surname, First name: *Title.* Publisher, place of publication, year of publication [year of original publication].	Clausewitz, Carl von: *Vom Kriege.* Nikol Verlag, Hamburg, 2008 [1832].	
Hungarian, Japanese, Korean, Vietnamese, etc. author	Surname, First name: *Title.* Publisher, place of publication, year of publication.	Fabian, Sandor: *Professional Irregular Defense Forces: the other Side of COIN.* Master's Thesis, Naval Postgraduate School, 2012. The customary sequence of names in some countries (e.g., Hungary, Japan, etc.) is surname, given names. For consistency in the appearance of the bibliography, use a comma after the surname.	Fabian 2012.
Work of unknown/ unidentifiable author	*Title.* Publisher, place of publication, year of publication.	*Guide to the Sources of Asian History.* National Archives of India, New Delhi, 1997.	Sources of Asian History, 1997. Shorten the title, and do not italicise.
Published work with bibliographic datum missing	*Title.* Publisher, place of publication, year of publication.	Indicate the missing data with square brackets: [no publisher], [no place], [no year].	
Repeated citations		The use of Latin abbreviations (ibid., op. cit., etc.) is discouraged.	Last name, year, page if necessary.
Radio Show/ Podcast	Host/Performer: *Program title.* Radio/Website, publication date. URL (Date of Download).	Lopez, Ashley: *After Nevada's primaries, voters in the state say they're frustrated.* National Public Radio. https://www.npr.org/2024/02/07/1229723059/after-nevadas-primaries-voters-in-the-state-say-they-re-frustrated 02/07/2024 (Downloaded: 02/05/2024).	Lopez: After Nevada… 2024. Shorten long titles.
TV show	*Program Title.* Channel Name, publication date. URL (Date of Download).	*The tiny German island with a population of 16.* BBC, 07/15/2019. https://www.bbc.com/reel/video/p07cjvmc/the-tiny-german-island-with-a-population-of-16 (Downloaded: 02/05/2024).	Tiny German Island… 2019. Shorten long titles.
YouTube	Username [@ nickname] (year of publication): *Title.* YouTube, publication date. URL (Date of Download).	Lindybeige [@lindybeige] (no year): *Republican Roman Soldiers of the Second Punic War.* YouTube, no date. https://www.youtube.com/watch?v=TeU8pXr0ucI (Downloaded: 02/05/2024).	Lindybeige: Republican Roman Soldiers… no year. Shorten long titles.

Reference formatting requirements			
type of work cited	**content of citation**	**in bibliography**	**in footnote**
Social media	User [@nickname]: *Title* or first few words of post. Media name, date of publication. URL (Date of Download).	NOELREPORTS [@NOELreports]: The US Army aims to double the production… Twitter, 02/06/2024. https://twitter.com/NOELreports/status/1754777264674254944 (Downloaded: 02/06/2024).	NOELREPORTS 02/06/2024
Movie	*Movie title*. (Genre) Reg. Director's name. Manufacturer, year of publication.	*Alphaville: A Strange Adventure of Lemmy Caution*. (distopian science fiction) Director: Jean-Luc Godard. Athos Films, 1965.	Alphaville 1965.
Laws, articles of law, decrees, ordinances		The Disturbed Areas (Special Courts) Act 1976, Act No. 77 of 1976. Article 3. Section (2). Act of the Parliament of the Republic of India. Title and number of the legislation, type of legislation, year of promulgation, article and section, as appropriate. Sequence the identifying information as close to the original as possible, use Roman or Arabic numerals as in the original.	Disturbed Areas Act 1976.

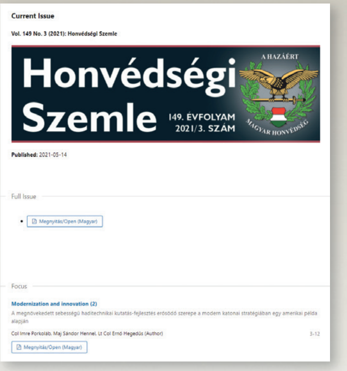
You can read the articles of HONVÉDSÉGI SZEMLE and HUNGARIAN DEFENCE REVIEW online!

kiadvany.magyarhonvedseg.hu/index.php/honvszemle/

The brand new issues of Honvédségi Szemle and Hungarian Defence Review are available at: kiadvany.magyarhonvedseg.hu/index.php/honvszemle/

Just click on the link and you can immediately read the articles of our latest publications and even the full content of our current issue. Click on each study to find out more about our authors and to learn which of our journals are the most popular. If you are interested in reading about current military issues, you can also find them under News.

In addition, you can learn about our editorial board and editorial staff, our guidelines for authors, our reviewing process, ethics and privacy statement and our archiving policy – all of which have made our page a significant journal.



Current Issue

Vol. 149 No. 3 (2021): Honvédségi Szemle

Published: 2021-05-14

Full Issue

- Megnyitás/Open (Magyar)

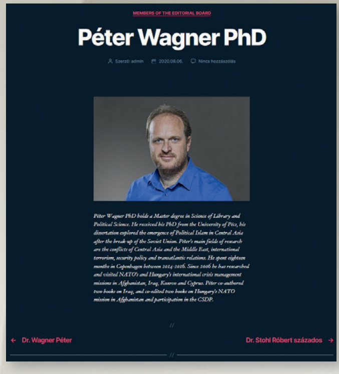
Focus

Modernization and innovation (2)

A megnövekedett sebességű haditechnikai kutatás-fejlesztés erősödő szerepe a modern katonai stratégiában egy amerikai példa alapján

Col Imre Porkoláb, Maj Sándor Hennel, Lt Col Ernő Hegedűs (Author) 3-12

Megnyitás/Open (Magyar)



MEMBERS OF THE EDITORIAL BOARD

Péter Wagner PhD

Szerző: admin 2020.08.06. Nincs hozzászólás

Péter Wagner PhD holds a Master degree in Science of Library and Political Science. He received his PhD from the University of Pécs, his dissertation explored the emergence of Political Islam in Central Asia after the break-up of the Soviet Union. Péter's main fields of research are the conflicts of Central Asia and the Middle East, international terrorism, security policy and transatlantic relations. He spent eighteen months in Copenhagen between 2014-2016. Since 2006 he has researched and visited NATO's and Hungary's international crisis management missions in Afghanistan, Iraq, Kosovo and Cyprus. Péter co-authored two books on Iraq, and co-edited two books on Hungary's NATO mission in Afghanistan and participation in the CSDP.

← Dr. Wagner Péter

Dr. Stohl Róbert százados →

Hungarian Defence Review
HONVÉDSÉGI SZEMLE

About Us Current Issue Archives Guidelines Military News Events

Home / Archives / Vol. 149 No. 3 (2021): Honvédségi Szemle / Focus

Modernization and innovation (2)

A megnövekedett sebességű haditechnikai kutatás-fejlesztés erősödő szerepe a modern katonai stratégiában egy amerikai példa alapján

Col Imre Porkoláb
Maj Sándor Hennel
Lt Col Ernő Hegedűs

DOI: https://doi.org/10.35926/HSZ.2021.3.1

Keywords: military strategy, military research and development, digitization, virtual test, Multi Domain Operation, hybrid warfare, offset strategy, transformation, military science model, "e" series

Abstract

The study draws attention to the fact that innovation is a strategic tool. An important component of defense innovation is to align the latest advances in the technological revolution with the objectives of force development. Therefore, this study analyses the relationship between modern military strategy and innovation by examining the effects of the latest, digitized method of military technology research and development through a case study. The effect of the new development methodology is that the military technology research and development project cycle significantly accelerates, which not only allows us to seize the technological advantage in the near future, but also to create strategic surprises and a lasting strategic competitive advantage by creating completely new weapon systems and thereby maintaining a lasting strategic competitive advantage. In this way, a new type of military technology research and development process built on a significant IT base will become a key element of the military strategy of the future.

Author Biographies

Col Imre Porkoláb
Col Imre Porkoláb PhD is the chief of the Editorial Board, Hungarian Defence Review

Maj Sándor Hennel
Maj Sándor Hennel, PhD is the senior officer of HDF 808 32. National Parade Unit.
ORCID

Lt Col Ernő Hegedűs
Lt Col Ernő Hegedűs, PhD is an assistant professor at University of Public Service, Budapest.
ORCID

Honvédségi Szemle

Megnyitás/Open (Magyar)

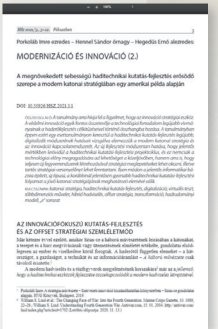
Published
2021-05-13

How to Cite
Porkoláb, I., Hennel, S., & Hegedűs, E. (2021). Modernization and innovation (2): A megnövekedett sebességű haditechnikai kutatás-fejlesztés erősödő szerepe a modern katonai stratégiában egy amerikai példa alapján. Honvédségi Szemle – Hungarian Defence Review, 149(3), 3-12. https://doi.org/10.35926/HSZ.2021.3.1

More Citation Formats

Issue
Vol. 149 No. 3 (2021): Honvédségi Szemle

Section
Focus



HSz 2021/3. 3–12. Fókuszban 3

Porkoláb Imre ezredes – Hennel Sándor őrnagy – Hegedűs Ernő alezredes:

MODERNIZÁCIÓ ÉS INNOVÁCIÓ (2.)

A megnövekedett sebességű haditechnikai kutatás-fejlesztés erősödő szerepe a modern katonai stratégiában egy amerikai példa alapján

DOI: 10.35926/HSZ.2021.3.1

ÖSSZEFOGLALÓ: A tanulmány arra hívja fel a figyelmet, hogy az innováció stratégiai eszköz. A védelmi innováció egyik fontos összetevője a technológiai forradalom legújabb vívmányainak a haderőfejlesztés célkitűzéseivel történő összhangba hozása. A tanulmányban éppen ezért egy esettanulmányon keresztül a haditechnikai kutatás-fejlesztés legújabb, digitalizált módszerének hatásait vizsgálva elemezzük a modern katonai stratégia és az innováció kapcsolatrendszerét. Az új fejlesztési módszertan hatása, hogy jelentős mértékben lerövidül a haditechnikai kutatási-fejlesztési projektciklus, és ez nemcsak a technológiai előny megragadására ad lehetőséget a közeljövőben, hanem arra is, hogy teljesen új fegyverrendszerek létrehozásával stratégiai meglepetéseket lehet okozni, illetve tartós stratégiai versenyelőnyt lehet fenntartani. Ilyen módon a jelentős informatikai bázisra épített, új típusú, a korábbinál jelentősen gyorsabb haditechnikai kutatási-fejlesztési folyamat a jövő katonai stratégiájának meghatározó elemévé válik.

KULCSSZAVAK: katonai stratégia, haditechnikai kutatás-fejlesztés, digitalizáció, virtuális teszt, többdimenziós művelet, hibrid hadviselés, offset stratégia, transzformáció, hadtudományi modell, „e" sorozat

AZ INNOVÁCIÓFÓKUSZÚ KUTATÁS-FEJLESZTÉS ÉS AZ OFFSET STRATÉGIAI SZEMLÉLETMÓD

Már kétezer évvel ezelőtt, amikor Szun-ce a háború művészetének leírásában a katonákat, a terepet és a harc megvívásának vagy ütemezésének elméletét értékelte, gondolatai elsődlegesen az ember és viselkedése körül forogtak. A haderőtől független elemeket – a hátországot, a gazdaságot, a technikát és az információáramlást – *A háború művészete* csak távolról érintette.[1]

A modern hadviselés és a tűzfegyverek megjelenésének korszakára[2] már az a *jellemző, hogy a haditechnikai eszközök fejlesztése összekapcsolódik a modern hadviselés létrejöttével.*

[1] Porkoláb Imre: A stratégia művészete – Szervezeti innováció kiszámíthatatlan környezetben – Szun-ce gondolatai alapján. HVG Könyvek, Budapest, 2019.

[2] William S. Lind et al.: The Changing Face of War: Into the Fourth Generation. Marine Corps Gazette, 10. 1989, 22–26.; William S. Lind: Understanding Fourth Generation War. Antiwar.com, 15. 01. 2004. http://antiwar.com/lind/index.php?articleid=1702 (Letöltés időpontja: 2020. 11. 13.)

If you want to be informed about our latest issue in time, just sign up now and we'll send you the content of our next issue before it's released!

We wish you a pleasant reading.
The Editorial Staff

ZRÍNYI KIADÓ