VOJENSKÉ REFLEXIE

DOI: https://doi.org/10.52651/vr.j.2025.3

AOS military science journal AOS

VOLUME XX
ISSUE 3/2025

AKADÉMIA OZBROJENÝCH SÍL
GENERÁLA MILANA RASTISLAVA ŠTEFÁNIKA

Armed Forces Academy
of Gen. Milan Rastislav Štefánik

VOJENSKÉ REFLEXIE

MILITARY SCIENCE JOURNAL

VOLUME XX
ISSUE 3/2025

ARMED FORCES ACADEMY OF GENERAL MILAN RASTISLAV ŠTEFÁNIK LIPTOVSKÝ MIKULÁŠ
Editorial board

EDITORIAL OFFICE
EDITOR-IN-CHIEF:

Assoc. Prof. Eng. Ivan MAJCHÚT, PhD.

MEMBERS:

Eng. Soňa JIRÁSKOVÁ, PhD., Cpt. Eng. Miriam KARASOVÁ, Eng. Dušan SALAK, Mgr. Katarína HOLOŠOVÁ

Journal is indexed in ERIHPLUS, DOAJ

ISSN 1336-9202

Editorial Board address
Akadémia ozbrojených síl generála Milana Rastislava Štefánika
Demänová 393, 031 01 Liptovský Mikuláš
tel. +421 960 423524, +421 960 422620
e-mail redakcie / e-mail board: lubomir.belan@aos.sk; ivan.majchut@aos.sk

Published papers did not undergo language correction.
The content, the professional, and language levels of the papers are in the full responsibility of the authors.

The peer-reviewed journal Vojenské reflexie was established in 2006 and is issued by the Armed Forces Academy, which is a state military university with a long history of **scientific research in the field of security, defence and the military**. At present, the academy cooperates with partners from military and civilian universities and other renowned specialized institutions from the Slovak Republic as well as from abroad.

The journal Vojenské reflexie is intended for contributors and readers from the security community, members of the armed forces, academic teachers, students and other readers interested in the following:

- **security and strategic studies,**
- **operational art and tactics,**
- **economy and management of defence resources,**
- **socialstudies and humanities,**
- **political science and international affairs,**
- **military technologies and technological studies,**
- **military and police theory and practice,**
- **lifelong and career education.**

Opinions and attitudes presented in the articles do not necessarily have to be in accordance with the opinion of the editor and the editorial board of the journal. They are the sole responsibility of their authors. The journal does not charge article processing or any other charges.

The articles are published in Slovak, Czech and English language. The articles are peer-reviewed. The journal Vojenské reflexie is published in electronic format on its website: vr.aos.sk :

- Twice a year in Slovak and Czech language, always in June and December

- Once a year in English, always in December.

Vojenské reflexie is a journal with open access, which means that the whole content is available for the readers or institutions for free. The readers may read, download, copy, distribute, print or refer to the texts of the articles or use them for any purpose without the consent of the authors or editor. The readers may copy, distribute and refer to the articles when citing the source.

Reviewers

Prof. Eng. Andrej Veľas, PhD.,

University of Zilina,
Zilina, Slovakia

Assoc. Prof. Eng. Rtd. Col. Radoslav IVANČÍK, PhD. et PhD., MBA, MSc.,

Constantine The Philosopher University in Nitra,
Nitra, Slovakia

Assoc. Prof. JUDr. MUDr. Daniel ŠMIHULA, PhD., Dr. Iur.,

Ministry of Foreign and European Affairs of the Slovak Republic,
Bratislava, Slovakia

Assoc. Prof. Eng. Vladimír ANDRASSY, PhD.,
Col. Eng. Jaroslav KOMPAN, PhD.,
Assoc. Prof. Eng. Ivan MAJCHÚT, PhD.,
Assoc. Prof. Eng. Stanislav MORONG, PhD.,
Lt. Col. Eng. Milan TURAJ, PhD.,
PhDr. Miroslav ŠPÁNIK, PhD.,
Eng. Rudolf PÁSTOR, PhD.,
Eng. Marián ŠIMON,
Eng. Michal VAJDA

Armed Forces Academy of general Milan Rastislav Štefánik,
Liptovský Mikuláš, Slovakia

Assoc. Prof. RSDr. Jozef MATIS, PhD.,
Assoc. Prof. PhDr. Mária PETRUFOVÁ, PhD.

Liptovský Mikuláš, Slovakia

CONTENTS

DOI: https://doi.org/10.52651/vr.a.2025.3.7-17
VOJENSKÉ REFLEXIE
ISSN: 1336-9202 (online)
2025, Number 3, Page 7-17

TACTICAL NUCLEAR WEAPONS IN CONTEMPORARY MILITARY STRATEGY: RISKS, CAPABILITIES, AND DOCTRINAL EVOLUTION

ZOLTÁN ŐZE

ARTICLE HISTORY

Submitted: *19. 12. 2024*
Accepted: *27. 11. 2025*
Published: *31. 12. 2025*

ABSTRACT

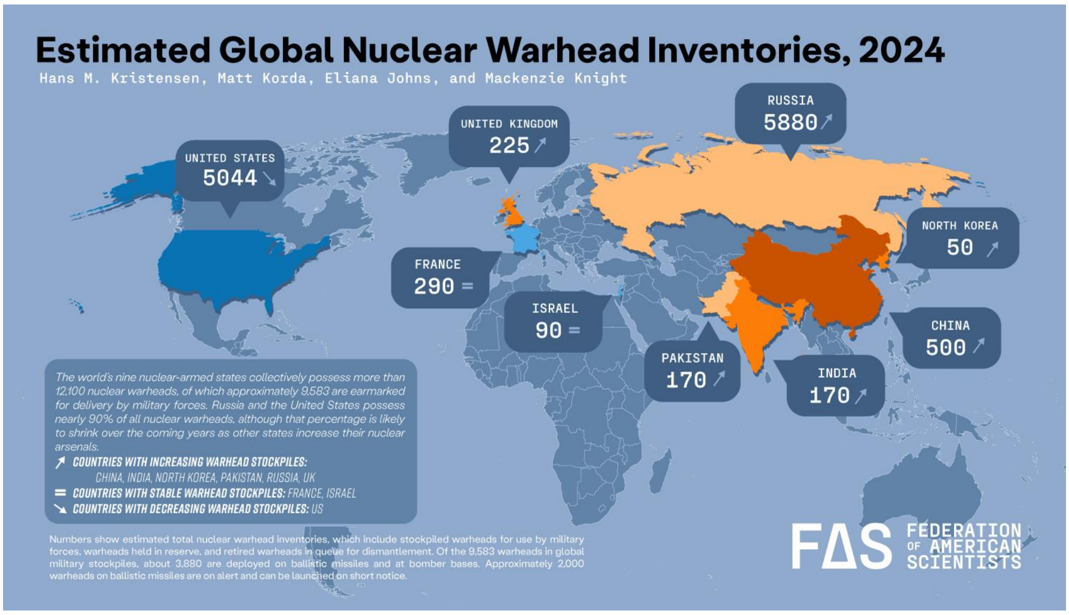
Recent geopolitical tensions—especially the Russian-Ukrainian conflict—have revived concerns regarding tactical nuclear weapons. This paper explores the blurred line between tactical and strategic nuclear weapons, examining their capabilities, doctrinal relevance, and current deployment status. Through qualitative analysis based on open-source intelligence and official defense publications, the study identifies key developments in Russia's tactical nuclear arsenal, NATO's defensive posture, and the United States' modernization efforts. The paper concludes that while the probability of actual nuclear use remains low, the proliferation and doctrinal normalization of tactical nuclear weapons constitute a serious threat to international security in the 21st century.

KEYWORDS

tactical nuclear weapons, nuclear strategy, proliferation, deterrence, escalation, Russian doctrine, NATO

INTRODUCTION

In January 2022, the five recognized nuclear-armed states and permanent members of the United Nations Security Council—China, France, Russia, the United Kingdom, and the United States—issued a joint statement affirming that "a nuclear war cannot be won and must never be fought." (The White House, 2022). This echoes a historic declaration first made in 1985 by U.S. President Ronald Reagan and Soviet General Secretary Mikhail Gorbachev. (Ronald Reagen Presidental Library & Museum, 1985) In that year, the Soviet Union was estimated to secure world peace with almost 40 000 nuclear warheads, and the US with more than 23 000 (Global Nuclear Stockpiles 1945-1997, 1997).This number is now less than six thousand for both forces (Figure 1).



Estimated Global Nuclear Warhead Inventories, 2024

Hans M. Kristensen, Matt Korda, Eliana Johns, and Mackenzie Knight

The world's nine nuclear-armed states collectively possess more than 12,100 nuclear warheads, of which approximately 9,583 are earmarked for delivery by military forces. Russia and the United States possess nearly 90% of all nuclear warheads, although that percentage is likely to shrink over the coming years as other states increase their nuclear arsenals.

↗ COUNTRIES WITH INCREASING WARHEAD STOCKPILES: CHINA, INDIA, NORTH KOREA, PAKISTAN, RUSSIA, UK

= COUNTRIES WITH STABLE WARHEAD STOCKPILES: FRANCE, ISRAEL

↘ COUNTRIES WITH DECREASING WARHEAD STOCKPILES: US

Numbers show estimated total nuclear warhead inventories, which include stockpiled warheads for use by military forces, warheads held in reserve, and retired warheads in queue for dismantlement. Of the 9,583 warheads in global military stockpiles, about 3,880 are deployed on ballistic missiles and at bomber bases. Approximately 2,000 warheads on ballistic missiles are on alert and can be launched on short notice.

Figure 1. Number of Nuclear Warheads in the world 2024
Source: *(Kristensen, et al., 2024)*

Despite such commitments, the current international security environment reveals increasing nuclear posturing, especially concerning the use of tactical nuclear weapons.

During the Cold War, the balance of terror was maintained through the doctrine of mutually assured destruction, primarily involving strategic nuclear arsenals. Today, however, a renewed focus on tactical nuclear weapons—smaller, more flexible, and battlefield-oriented nuclear arms—is reshaping nuclear deterrence strategies. Russian military doctrine, in particular, reflects a lowering of the nuclear threshold, and exercises involving simulated use of TNWs have become more frequent. At the same time, the United States and NATO have modernized their limited tactical capabilities in response.

This article examines the evolving role of tactical nuclear weapons in modern military doctrines. It addresses key definitional challenges, analyzes current deployment patterns, and assesses the risks associated with their potential use. By placing these developments in historical and strategic context, the study aims to clarify how tactical nuclear weapons influence deterrence, escalation dynamics, and international security.

1 METHODS

This study employs a qualitative, document-based analytical approach, drawing on a wide range of primary and secondary sources. Key data points are extracted from official reports published by national defense institutions—including the U.S. Department of Defense and NATO—alongside strategic analyses by think tanks such as the Federation of American Scientists and the International Institute for Strategic Studies. Historical data on nuclear arsenals are drawn from declassified archives and peer-reviewed academic literature.

The methodology includes comparative analysis to evaluate the evolving doctrines and deployment strategies of tactical nuclear weapons in different nuclear-armed states. Particular emphasis is placed on the Russian Federation, the United States, and NATO allies, whose nuclear postures and capabilities represent the most dynamic areas of development in the post-Cold War era. The study also mentions very limited elements of game theory to interpret deterrence logic and escalation risks, especially in crisis scenarios involving potential tactical nuclear use.

To complement doctrinal analysis, the paper reviews current nuclear modernization programs and regional deployments, such as forward-basing in Europe and weapons storage near Russia's western borders. Open-source satellite imagery and intelligence assessments are referenced when relevant to support claims about deployment readiness.

2 RESULTS

The analysis reveals several key developments regarding tactical nuclear weapons (TNWs) in the 21st century:

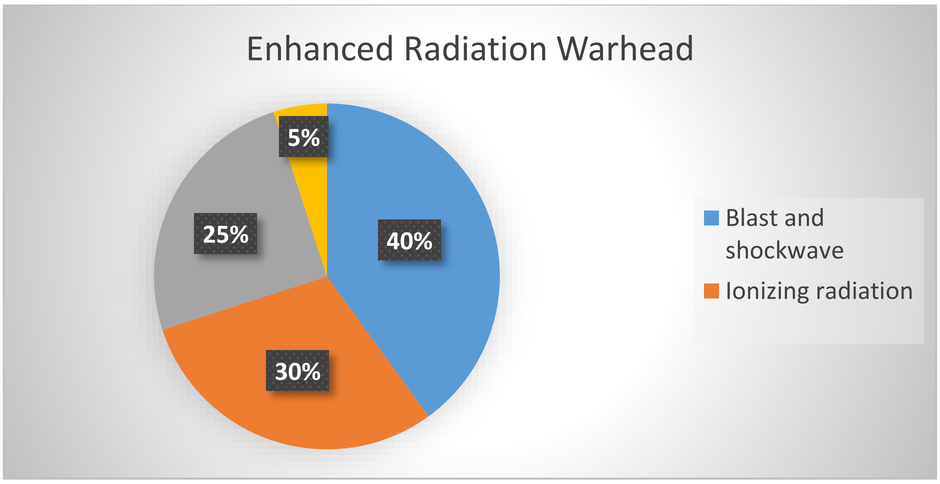
1. Russian tactical superiority and forward storage: Russia possesses the largest and most diversified arsenal of TNWs, estimated at nearly 2,000 warheads. These are believed to be stored in dozens of central facilities, with some near conflict zones such as the Ukrainian border (e.g., Belgorod). While not kept on constant alert, Russian TNWs can be prepared for deployment within hours or days, posing a serious challenge to early-warning systems.
2. Doctrinal shifts and use thresholds: Russia’s military doctrine increasingly integrates TNWs into conventional scenarios, suggesting their potential use to de-escalate conflicts on favorable terms. This is reinforced by recurring nuclear signaling during military exercises and public statements by top officials.
3. U.S. and NATO modernization efforts: In contrast, the United States currently deploys around 230 tactical nuclear weapons, all of which are gravity bombs (B61 variants), with approximately 150 stationed in five NATO member states. Recent modernization programs include the W76-2 low-yield warhead on Trident submarine missiles, and the B61-12 upgrade for enhanced precision.
4. Technological alternatives to tactical nuclear use: Advances in precision-guided conventional munitions have reduced the strategic utility of TNWs in Western military doctrines. NATO has gradually eliminated most TNWs from its stockpile, favoring non-nuclear deterrence tools and strategic ambiguity.
5. Proliferation and risk of escalation: The relative portability and lower political barrier to using TNWs increase the risk of limited nuclear exchanges, especially in regional conflicts. Despite their smaller yields, TNW use would likely result in massive civilian casualties and uncontrollable escalation.

3 DISCUSSION

The resurgence of tactical nuclear weapons (TNWs) in contemporary military strategy represents a fundamental challenge to the long-standing norms of nuclear deterrence and escalation management. The Cold War deterrence model relied on strategic nuclear weapons with high yields and guaranteed second-strike capabilities, thereby creating a clear threshold against nuclear use. In contrast, TNWs blur the distinction between nuclear and conventional warfare due to their lower yield, shorter range, and flexible deployment options.

For military purposes, the Enhanced Radiation Warhead also known as neutron bomb is best suited for the destruction of life forces, a special type of small thermonuclear weapon that produces minimal light and heat effects but emits large amounts of lethal radiation (Figure 2). A neutron weapon differs from a conventional nuclear weapon in that its primary effect is the adverse physiological effects caused by the neutrons it emits (Medical Implications of Enhanced Radiation Weapons, 2010).

The shockwave has a lower energy, so physical structures, including houses and industrial installations, are less affected. Because the effects of neutron radiation diminish very rapidly with distance, much smaller areas are exposed to lethal levels of radiation (A Comparison of the Effects of Neutron Bombs and Standard Fission Weapons, 1981).



Graph 1. Enhanced Radiation Weapons’effects
Source: (Enhanced Radiation Weapons, 1978)

Because of its relatively small strike area, the neutron weapon would be highly effective against tank units and infantry on the battlefield, but would not threaten cities or other structures within a few kilometers. The American scientist Samuel Cohen[1], who died in 2010, developed the concept of the weapon (Cohen, 1978).

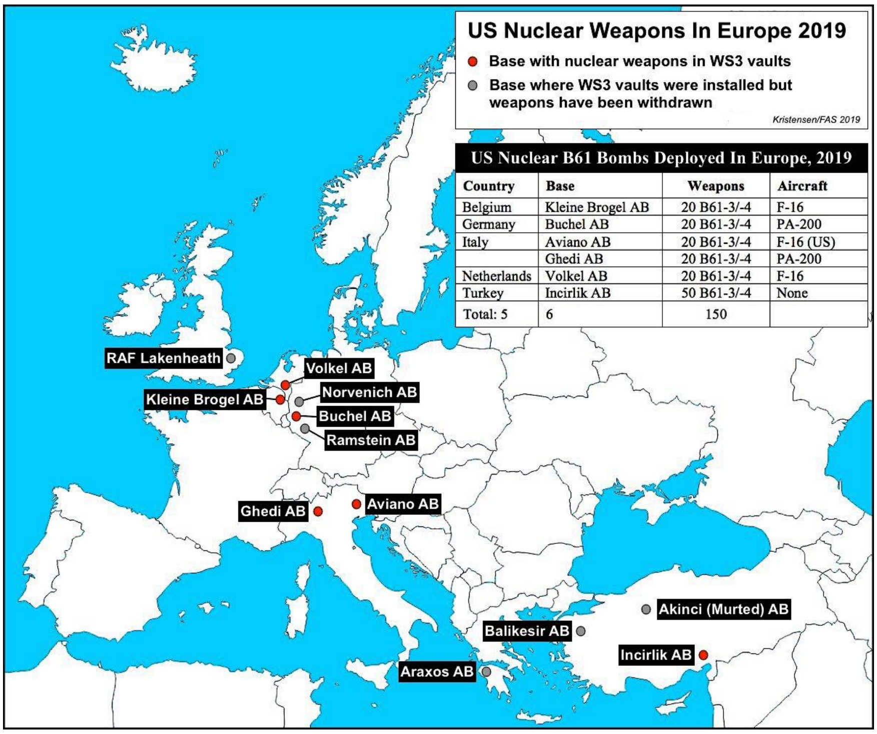
[1] Samuel T. Cohen (Brooklyn, January 25, 1921 – Los Angeles, November 28, 2010) was an American physicist. In 1947, he joined RAND and worked as a consultant at the Lawrence Livermore National Laboratory. The RAND project was established by the United States Air Force to research the weapons of the future. In 1958, Cohen developed the neutron bomb here.

The neutron bomb was designed to stop a possible invasion of Western Europe by Soviet forces. Currently, the technologies to create an Enhanced Nuclear Warhead are owned by the United States, Russia and China (possibly France). In the 1980s, the US had 20-30,000 tactical nuclear weapons and the Soviet Union had about 13-22,000 (Global Nuclear Stockpiles 1945-1997, 1997).

The United States of America stationed most of its warheads in Western Europe, because then it was part of the American military doctrine what the Russians have now: if conventional forces fail to stop the enemy, then nuclear weapons can come in.

During the Cold War, the Warsaw Pact's conventional troops were outnumbered in Europe, which the US countered with missile deployments that provoked protests from the population in many places. However, with the collapse of the Soviet Union, the Warsaw Pact was dissolved, NATO was enlarged, and the balance of power was reversed, with conventional supremacy shifting to NATO.

This is reflected in the fact that the US now has only about 230 tactical nuclear weapons, all of them aircraft-launched (B61 family), conventional nuclear bombs, and an estimated 150 of them are in Europe - divided between the five countries with six US bases - Belgium (Kleine Brogel), Germany (Brüchel), Italy (Aviano and Ghedi), the Netherlands (Volkel) and Turkey (Incirlik) (Graph 2). NATO largely eradicated its tactical nuclear stockpile after the end of the Cold War mainly because in the meantime, military technology has evolved to the point where conventional weapons are more precise - especially artillery and missiles – and they are able to perform similar tasks more cheaply and with less complication.



US Nuclear B61 Bombs Deployed In Europe, 2019

Country	Base	Weapons	Aircraft
Belgium	Kleine Brogel AB	20 B61-3/-4	F-16
Germany	Buchel AB	20 B61-3/-4	PA-200
Italy	Aviano AB	20 B61-3/-4	F-16 (US)
	Ghedi AB	20 B61-3/-4	PA-200
Netherlands	Volkel AB	20 B61-3/-4	F-16
Turkey	Incirlik AB	50 B61-3/-4	None
Total: 5	6	150	

Graph 2. The U.S. nuclear weapons in Europe in 2019
Source: (Kristensen, 2019)

The UK − which now only has submarine-launched ballistic missiles − and France do not have tactical nuclear weapons, although the French's air-launched devices have similar characteristics.

Meanwhile, a US congressional report estimates that Russia still has almost 2,000 (Woolf, 2022) tactical nuclear weapons, and an increasing number of them are modernized, such as the Iskander missile-mounted version (Figure 2) that is also deployed in the Kaliningrad enclave between Poland and Lithuania.

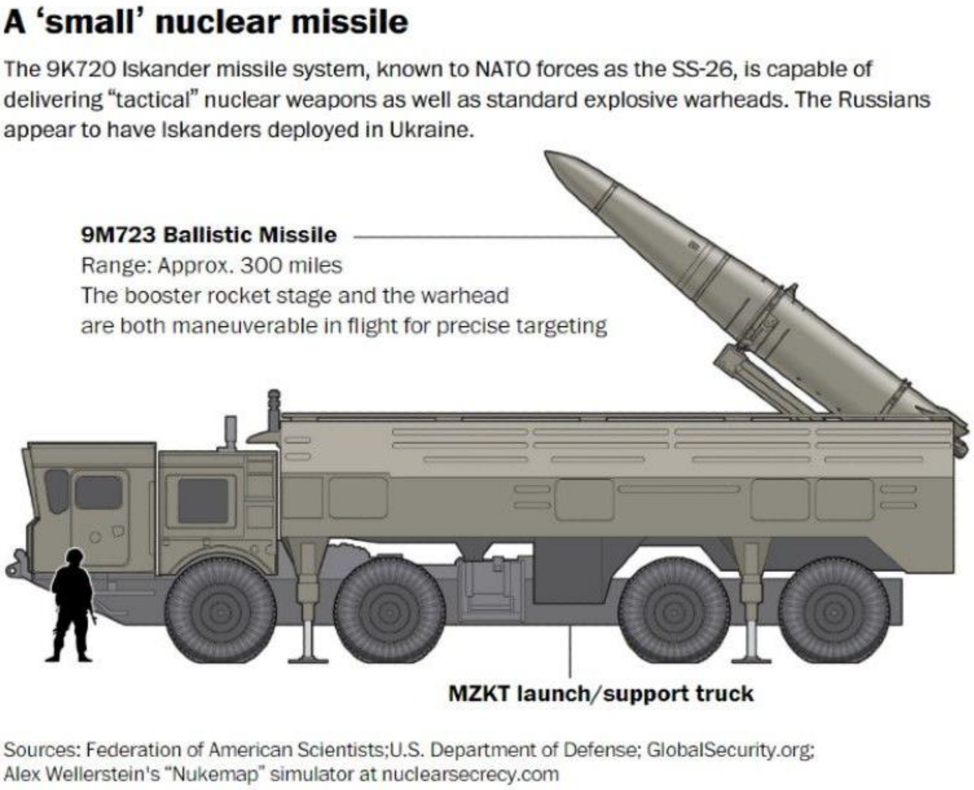

A 'small' nuclear missile
The 9K720 Iskander missile system, known to NATO forces as the SS-26, is capable of delivering "tactical" nuclear weapons as well as standard explosive warheads. The Russians appear to have Iskanders deployed in Ukraine.
9M723 Ballistic Missile
Range: Approx. 300 miles
The booster rocket stage and the warhead are both maneuverable in flight for precise targeting
MZKT launch/support truck
Sources: Federation of American Scientists;U.S. Department of Defense; GlobalSecurity.org; Alex Wellerstein's "Nukemap" simulator at nuclearsecrecy.com

Figure 2. Technical data of the Iskander missile, which can also be equipped with the AA-60 warhead (yield of 10–100 Kt)
Source: (BBC News, 2022)

Shortly after the turn of the millennium, Moscow started to modernize its nuclear arsenal and delivery systems on Putin's orders. In the face of Russian efforts, and following the annexation of Crimea, Barack Obama launched the US modernization program, which is expected to last up to 30 years and cost at least 1.5 trillion dollars (Bennett, 2023).

It was the next US president, Trump, who ordered the development of warheads that could be mounted on Trident missiles used on submarines, and the W76-2, which can scale between 25 and 100 kilotons, was completed relatively quickly and was deployed in January 2020 (Mehta, 2020).

During the Cold War, tens of thousands of warheads kept NATO and the Warsaw Pact member countries from using nuclear weapons against each other through mutually assured destruction, because escalation threatened the total annihilation of human civilization -

which, fortunately, has only happened in science fiction novels. The mechanism of nuclear deterrence can be derived mathematically using game theory methodology. The best example of this is the Cuban Missile Crisis, a study of which mathematically deduces exactly why nuclear apocalypse did not occur in 1962 (Shaabani, et al., 2023).

But the threat appears to be resurgent, with Vladimir Putin announcing the deployment of nuclear weapons in the event of an attempted intervention by an outside power during his invasion of Ukraine (Cimbala, et al., 2024). The Russian rhetoric is most likely to threaten with so-called "tactical nuclear weapons", which differ in range and purpose of deployment from strategic nuclear weapons (Tactical nuclear weapons, 2019). The distinction between tactical and strategic nuclear weapons is not straightforward and involves multiple factors:

- Range is often more important consideration than explosive power.
- The nature of the target and the weapon's intended use are also determining factors.
- Some experts argue that the "tactical" and "strategic" distinction is not useful, and that all nuclear weapons should be considered collectively.

The yield does not typically determine whether a nuclear weapon is classified as strategic or tactical - even if we can establish that it is not justified to use a high-yield nuclear weapon for tactical purposes (near friendly forces), while low-yield nuclear weapons can also achieve strategic effects. Indeed, the yield alone is not a decisive factor in categorizing a nuclear weapon as strategic or tactical. There are significant overlaps in the explosive power of tactical and strategic weapons. The classification of weapons is greatly influenced by their intended use: tactical weapons are generally designed for battlefield use, such as against large infantry formations or armored units while strategic weapons are intended more for attacking the enemy's homeland, cities, or strategic nuclear forces. According to Encyclopaedia Britannica the “tactical nuclear weapons, small nuclear warheads and delivery systems intended for use on the battlefield or for a limited strike” (Encyclopaedia Britannica). Technically, a tactical nuclear weapon is one that is not subject to the START agreements on strategic nuclear arms limitation.

However, a significant difference between tactical and strategic nuclear weapons is that strategic nuclear weapons are kept in constant readiness, because if the attack mechanism is activated at any time based on strictly controlled codes, the attacked country's retaliatory strike will arrive within minutes. Tactical nuclear weapons, on the other hand, are generally not ready for deployment. These devices are stored in central warehouses, there are dozens of such secret facilities in Russia, one of them happens to be right at the Ukrainian border, near the city of Belgorod, one of the launching points of the Russian invasion in February 2022 (Alberque, 2022). It would take a few hours or a few days to prepare the weapons for potential use, and in the present circumstances it is safe to assume that Western intelligence organizations are closely monitoring such actions.

Russian military doctrine is particularly notable in this context. The integration of TNWs into operational planning and their simulation in large-scale exercises reflect a doctrinal willingness to consider limited nuclear strikes in conventional conflict scenarios. This “escalate to de-escalate” approach carries significant risks: it reduces the psychological and strategic barriers to nuclear use and complicates adversaries' decision-making during crises. Moreover, Russian TNWs are not covered by strategic arms control treaties such as New START, making transparency and verification virtually impossible.

Meanwhile, the U.S. and NATO responses have been cautious but significant. While maintaining a much smaller TNW arsenal, modernization efforts such as the B61-12 and W76-2 reflect a shift toward credible, flexible deterrence. However, NATO’s current doctrine still prioritizes non-nuclear means, relying on advanced precision munitions and collective defense mechanisms rather than expanding its TNW stockpile.

The broader strategic implication is that the availability of TNWs may tempt political and military leaders to consider their use under the false assumption of limited consequences. Yet simulations and policy studies consistently show that any nuclear detonation—even of the lowest yield—would likely lead to rapid and potentially uncontrollable escalation. This raises profound ethical, humanitarian, and strategic concerns.

Furthermore, TNWs pose significant proliferation risks. As more states seek deterrence capabilities, the temptation to develop small-yield nuclear weapons may grow, particularly in volatile regions where full-scale nuclear arsenals are politically or technically unfeasible. The blurred threshold for use may also encourage rogue states or non-state actors to pursue tactical nuclear technologies.

CONCLUSION

Tactical nuclear weapons have re-emerged as a central issue in 21st-century military strategy, particularly in light of Russia’s assertive nuclear signaling and doctrinal flexibility. Although these weapons are often viewed as limited-use tools, their deployment carries substantial strategic and humanitarian risks. Unlike strategic weapons, TNWs are not constrained by international treaties, making their development and potential use harder to monitor and regulate.

In recent decades, Moscow has incorporated simulations of the use of tactical nuclear weapons into its major military exercises and has repeatedly renewed its military doctrine (Kofman, et al., 2021). In addition to that, leading Russian politicians regularly mention the possibility of using nuclear weapons (Pennington, et al., 2024). In response to the advisory opinion requested by the UN General Assembly in its resolution 49/75K, the 1996 resolution of the International Court of Justice in The Hague stated that the use or threat of use of nuclear weapons, although not directly regulated, is indirectly a form of aggression and cannot be used as a pre-emptive strike. (International Court of Justice, 1996)

For years, NATO has interpreted Russian military doctrine as permitting the use of tactical nuclear weapons to achieve military objectives by leveraging their deterrent effect and forcing the opponent to retreat (Daryl, 2022). The NATO Secretary General is also regularly required to issue statements regarding the deployment of Russian nuclear weapons in Belarus and NATO's nuclear deterrence capabilities (North Atlantic Treaty Organization, 2022).

However, simulations show that the use of a nuclear weapon, no matter how low the yield, can lead to a severe escalation and the loss of millions of lives. Moreover, although Putin regularly advocates the use of a tactical nuclear weapon − which many military experts say would not achieve any military advantage (Alberque, 2022) − it would only make himself and his country more pariah-like.

The findings of this study suggest that the existence and modernization of TNWs weaken the deterrent effect of mutually assured destruction by introducing the possibility of "limited" nuclear warfare. This creates dangerous ambiguity in escalation scenarios and undermines decades of arms control efforts. While the probability of tactical nuclear weapon use remains low, the mere possibility necessitates robust policy responses from the international community.

Unlike strategic nuclear arms, which are designed for large-scale deterrence and retaliation, tactical nuclear weapons serve battlefield purposes and often fall outside formal arms control agreements. Going forward, it is imperative for nuclear-armed states and alliances to develop clear policies, invest in verification mechanisms, and pursue arms control frameworks that include TNWs. Failure to address the risks associated with these weapons could lead to miscalculations with catastrophic consequences.

REFERENCES

A Comparison of the Effects of Neutron Bombs and Standard Fission Weapons. Scoville, Herbert Jr. 1981. 4, s.l. : Bulletin of Peace Proposals, 1981, Vol. 12. https://doi.org/10.1177/096701068101200413

Alberque, William. 2022. The International Institute for Strategic Studies. Russia is unlikely to use nuclear weapons in Ukraine. [Online] 10 10, 2022. https://www.iiss.org/online-analysis/online-analysis//2022/10/russia-is-unlikely-to-use-nuclear-weapons-in-ukraine.

BBC News. 2022. Ukraine war: Could Russia use tactical nuclear weapons? BBC News. [Online] 2022. https://www.bbc.com/news/world-60664169.

Bennett, Michael. 2023. Congressional Budget Office. Projected Costs of U.S: Nuclear Forces, 2023 to 2032. [Online] 07 2023. https://www.cbo.gov/system/files/2023-07/59054-nuclear-forces.pdf.

Cimbala, J. Stephen and Korb, J. Lawrence. 2024. Bulletin of The Atomic Scientists. Putin's nuclear warnings: heightened risk or revolving door? [Online] 03 28, 2024.

https://thebulletin.org/2024/03/putins-nuclear-warnings-heightened-risk-or-revolving-door/.

Cohen, Samuel. 1978. The neutron bomb, political, technological and military issues. USA : Institute for Foreign Policy Analysis, 1978.

Daryl, Kimball G. 2022. Arms Control Association. New Tactical Nuclear Weapons? Just Say No. [Online] 5 2022. https://www.armscontrol.org/act/2022-05/focus/new-tactical-nuclear-weapons-just-say-no.

Encyclopaedia Britannica. Britannica. tactical nuclear weapons. [Online] https://www.britannica.com/technology/nuclear-weapon.

Enhanced Radiation Weapons. Kaplan, M. Fred. 1978. 5, s.l. : Scientific American, 1978, Vol. 238. OTI ID 6539823. https://doi.org/10.1038/scientificamerican0578-44

Global Nuclear Stockpiles 1945-1997. Taylor & Francis online. 1997. 6, s.l. : Bulletin of the Atomic Scientists, 1997, Vol. 53. https://doi.org/10.1080/00963402.1997.11456792.

International Court of Justice. 1996. International Court of Justice. Legality of the Threat or Use of Nuclear Weapons. [Online] 1996. https://www.icj-cij.org/case/95.

Kofman, Michael, et al. 2021. Center for Naval Analysis. Russian Military Strategy: Core Tenets and. [Online] 08 2021. https://www.cna.org/reports/2021/08/Russian-Military-Strategy-Core-Tenets-and-Operational-Concepts.pdf.

Kristensen, Hans. 2019. Federation of American Scientists. Urgent: Move US Nuclear Weapons Out Of Turkey. [Online] 2019. https://fas.org/publication/nukes-out-of-turkey/.

Kristensen, Hans, et al. 2024. Federation of American Scientists. Status Of World Nuclear Forces. [Online] 03 29, 2024. https://fas.org/initiative/status-world-nuclear-forces/.

Medical Implications of Enhanced Radiation Weapons. Reeves, I. Glen. 2010. 12, s.l. : Military Medicine, 2010, Vol. 175. https://doi.org/10.7205/MILMED-D-10-00115

Mehta, Aaron. 2020. Defense News. Trump's new nuclear weapon has been deployed. [Online] 2 4, 2020. https://www.defensenews.com/smr/nuclear-arsenal/2020/02/04/trumps-new-nuclear-weapon-has-been-deployed/.

North Atlantic Treaty Organization. 2022. North Atlantic Treaty Organization. Press conference by NATO Secretary General Jens Stoltenberg following the extraordinary Summit of NATO Heads of State and Government. [Online] 2022. https://www.nato.int/cps/en/natohq/opinions_193613.htm?selectedLocale=en.

Pennington, Josh and Regan, Helen. 2024. CNN World. Putin says he's ready to use nuclear weapons if Russian state at stake, but 'there has never been such a need'. [Online] 3 2024. https://edition.cnn.com/2024/03/13/europe/russia-putin-nuclear-weapons-ukraine-intl-hnk/index.html.

Ronald Reagen Presidental Library & Museum. 1985. Ronald Reagen Presidental Library & Museum. [Online] 11 21, 1985. [Cited: 11 01, 2024.] https://www.reaganlibrary.gov/archives/speech/joint-soviet-united-states-statement-summit-meeting-geneva.

Shaabani, Somajeh and Gordji, Madjid Eshaghi. 2023. International Journal of Cuban Studies . GAME THEORY AND A NEW INSIGHT INTO HOW THE CUBAN MISSILE CRISIS WAS RESOLVED. [Online] 2023. https://www.jstor.org/stable/48728269?seq=7. https://doi.org/10.13169/intejcubastud.15.1.0039

Tactical nuclear weapons. Kristensen, M. Hans and Korda, Matt. 2019. 5, s.l. : Bulletin of the Atomic Scientists, 2019, Vol. 75. ISSN: 0096-3402. https://doi.org/10.1080/00963402.2019.1654273

The White House. 2022. The White House. Statements and releases. [Online] 01 03, 2022. [Cited: 11 20, 2024.] https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/03/p5-statement-on-preventing-nuclear-war-and-avoiding-arms-races/.

U.S. Departmment of Defense. 2023. media.defense.gov. Annual report to Congress. [Online] 2023. [Cited: 11 12, 2024.] https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

Woolf, Amy F. 2022. Russia’s Nuclear Weapons: Doctrine, Forces, and Modernization. [Online] 2022. https://sgp.fas.org/crs/nuke/R45861.pdf.

Zoltán ŐZE, Ph.D.
Address of workplace: H-1101 Budapest. 9-11 Hungária krt.
Telephone, fax. +36303283269
E-mail: oze.zoltan@uni-nke.hu

DOI: https://doi.org/10.52651/vr.a.2025.3.18-30
VOJENSKÉ REFLEXIE
ISSN: 1336-9202 (online)
2025, Number 3, Page 18-30

INFORMATION SECURITY OF THE PODKARPACKIE VOIVODESHIP IN THE FACE OF DISINFORMATION ACTIVITES OF THE RUSSIAN FEDERATION (2022-2025)

Piotr ZALEWSKI, Janusz KISZKA

ARTICLE HISTORY

Submitted: *26 09.2025*

Accepted: *27.11.2025*

Published: *31.12.2025*

ABSTRACT

The article analyses the nature, scale and effects of hybrid and disinformation activities directed at Polish with particular emphasis on the Podkarpackie Voivodeship in the years 2022–2025.

Based on a review of national and international reports, media analyses and case studies (cybersecurity incidents in local government offices, narratives about border crossings with Ukraine and Rzeszów-Jasionka airport, local information campaigns on refugees), the article identifies the main threat vectors, assesses regional vulnerabilities and formulates operational and strategic recommendations for regional authorities, local governments and NGOs.

KEYWORDS

Disinformation, hybrid warfare, cybersecurity, Russian Federation, regional information resilience.

INTRODUCTION

Information security is one of the key pillars of modern security on a national and regional scale. In the era of globalization, the flow of information has intensified and, thanks to new technologies and social media, it has become possible to quickly influence wide groups of recipients. This phenomenon, in addition to the obvious communication benefits, also raises serious security threats, including vulnerability to disinformation, information manipulation and hybrid actions aimed at the stability of states and societies. (Kancelaria Prezesa Rady Ministrów, 2023).

After the full-scale aggression of the Russian Federation against Ukraine in February 2022, Poland, as Kyiv's closest ally and a logistical and military hub to support the West, found itself in an unprecedented focus of attention for the activities of hostile services and propaganda centers (Menkiszak, 2022). The Podkarpackie region – bordering directly with Ukraine, with an extensive border and transport infrastructure (including the Rzeszów-Jasionka airport, rail, road and pedestrian border crossings in Medyka) was of particular importance, constituting facilities for humanitarian and military operations. The Russian Federation's hybrid actions towards Podkarpacie include both operations in cyberspace targeting local government institutions and critical infrastructure, as well as information operations aimed at shaping public opinion by spreading false narratives about the presence of allied troops, assistance to refugees, as well as the security of the region itself. The Kremlin, using its experience in conducting information wars, seeks to weaken public trust in state institutions, polarize society, as well as undermine Poland's credibility as a member of NATO and the European Union.

At the same time, the Podkarpackie region, due to its peripheral nature and limited resources of local governments in the field of cybersecurity and media education, is becoming particularly exposed to the effects of disinformation campaigns. Between 2022 and 2025, numerous examples of this type of activity were recorded, ranging from attempts to hack into the IT systems of municipal offices to organized narrative campaigns on social media aimed at inducing fear and information chaos.

The aim of the article is a comprehensive analysis of the nature, scale and effects of the Russian Federation's disinformation activities directed against the Podkarpackie Voivodeship in the years 2022-2025. The main research problem focuses on the question: how do the disinformation activities of the Russian Federation affect the information security of the Podkarpackie Voivodeship and what adaptation mechanisms are used by Russian propaganda campaigns in relation to specific local conditions? The thesis that the authors have tried to prove assumes that Russian disinformation activities against the Podkarpackie Voivodeship are characterized by a high degree of adaptation to specific local conditions, using in particular historical memory, social sensitivities and the strategic location of the region as a logistics hub for supporting Ukraine in the narrative used.

The study was conducted using methodological triangulation, combining qualitative analysis with elements of a quantitative approach. The following research methods and tools were used: analysis of documents and secondary sources - a systematic review of national and international reports on information security was carried out, including documents of the Centre for Strategic and International Studies (CSIS), reports of the European External Action Service (EEAS), analyses of the NATO Strategic Communications Centre of Excellence and CERT Polska documents concerning cybersecurity incidents; media analysis - systematic monitoring of publications in Polish and foreign media, social media platforms (Facebook, Twitter/X, Telegram) and news portals in the years 2022-2025 was used, with particular emphasis on content related to the Podkarpackie Voivodeship. Both official media publications and content published by users on social media were analyzed. Three key cases were selected for the case study and analysed in detail: 1. disinformation campaigns concerning refugees in Przemyśl in 2022, 2. manipulations related to the air incidents of September 2025, and 3. historical narratives using the memory of the Volhynia Massacre in the context of contemporary Polish-Ukrainian relations. For the narrative analysis, a discourse analysis method was used to identify the main narrative threads, rhetorical techniques, and persuasive strategies used in Russian disinformation campaigns.

The study covered the period from 24 February 2022 (the beginning of the Russian invasion of Ukraine) to September 2025. The territorial scope focuses on the Podkarpackie Voivodeship, with particular emphasis on border cities and municipalities, such as Przemyśl, Medyka, Korczowa and the functional area of the Rzeszów-Jasionka airport. The difficulties faced by the authors of the study were related to the limited availability of data on disinformation campaigns, due to their often classified nature. An important factor was also the dynamics of the analysed phenomena, which made it difficult to fully assess them over time, as well as the need to use only open data sources (OSINT) due to the lack of access to classified materials of the secret services. An important factor is also the "fog of war" that accompanies commanders, soldiers and researchers during military operations.

1 HAZARD CHARACTERISTICS

The years 2022–2025 were characterized by the intensification of the Russian Federation's hybrid activities towards Polish and, more broadly, towards NATO and EU countries. The turning point was Russia's invasion on Ukraine (February 2022), which triggered a wave of disinformation operations and cyberattacks targeting countries supporting Kyiv. Poland, due to its geopolitical location and key role in the logistics of support for Ukraine, has become the target of particularly intensive activities. Analyses by the CSIS and the EU's EEAS show that the number of manipulation operations and cyber-attacks has steadily increased and that their nature has become increasingly coordinated and multidimensional (Jones, 2024).

Russian disinformation was aimed at undermining trust in state and local government institutions, weakening support for Ukraine and creating a sense of threat among citizens. Social media (e.g. Facebook, X/Twitter, Telegram), low-credibility portals and bot networks were used for this. Narratives about the loss of sovereignty, the threats posed by refugees, and the alleged economic costs of the war played a special role.

In addition, cyberattacks are also used, which include both intelligence activities and sabotage attempts. The most commonly used are spear-phishing, software vulnerabilities and attacks on poorly secured systems of local government and public institutions. Some of the attacks were aimed at obtaining data for later information operations, e.g. publishing stolen documents in a manipulated form (CERT Polska, 2023).

In the analyzed period, cyberattacks were increasingly combined with information activities. The data obtained was selectively published in the media and then amplified by propaganda networks, which increased its credibility and reach. Such "mixed operations" increased the difficulty of identifying sources and complicated the state's response (Hybrid Threat Trends, 2024).

Due to the specific nature of the region's vulnerability, as a border region and logistics facilities for aid and military operations (Rzeszów-Jasionka airport, transport corridors, border crossings in Medyka, Korczowa), it has become the focus of interest of Russian activities. Local narratives focused, among others, on the alleged loss of control over the airport and the "militarization" of the region (FIMI Report, 2025).

An important aspect from the point of view of ensuring information security are the personnel and technological limitations of local governments. Many smaller municipalities in the Podkarpackie region have limited financial and human resources in the area of cybersecurity, which makes them vulnerable to attacks. Small local incidents could then be exploited in disinformation narratives (Financial Times, 2024). In addition, the region has a strong attachment to tradition and local identity, which has been used in disinformation narratives. Historical and national themes were often invoked to create antagonism towards refugees and NATO's activities.

In the short term, hybrid intensity is expected to remain high. We should expect an increasing combination of cyberattacks with disinformation, a wider use of AI-based tools for content generation, and further adaptation of narratives to the local context (e.g. concerns about border security and the economic costs of war).

2 ANTI-EMIGRATION NARRATIVES IN PRZEMYŚL (2022)

In the first weeks of the war, false information about crimes allegedly committed by refugees was spread online. This content was exaggerated or completely fabricated and was intended to provoke social unrest and anti-Ukrainian sentiment. According to fake news in Przemyśl, "dark-skinned refugees raped women" (Bednarek, 2022). The purpose of this fake news was to "build a sense of danger" or pro-Russian statements. As a result of disinformation activities, a dangerous rumor began to spread that dark-skinned refugees - by default, not directly affected by the war - began to attack Polish women and even rape them. A false message about the potential danger posed by refugees from African and Asian countries crossing the Polish-Ukrainian border circulated online for several days before escalating. Disinformation was reproduced and disseminated in a professional manner in order to arouse violent social emotions. However, the mere sowing of content in social media would not have provoked a strong reaction if it had not been for the fact that the topic was picked up by far-right circles. As a result, in Przemyśl, "patrols" of pseudo-fans organized, as one of the residents called it, a "hunt" for people with darker skin color.

The first reports of refugees from outside Ukraine were visible on social media as early as February 26. They were most often published by anonymous accounts. Among them were screenshots from private correspondence (without naming the authors), for example, with the following content: "Maybe you will be able to publicize the case, you have a greater reach... I have contact with a friend from Lviv, who wrote that Poles should not be deceived because black people are following the crowd of Ukrainian refugees... y from the Belarusian border (Iran, Iraq, Egypt, Turkey). I contacted my friends from customs, they were ordered by the government to let them through without verification (...) they trample women and children, one of them allegedly did not survive...". More and more of them appeared by the hour. They circulated on: Twitter, Telegram, Facebook, Messenger.

It was this impression that was used to build the belief that there are a lot of refugees from Africa and Asia on the border (Mierzwińska, 2022). In fact, citizens of non-European countries were also fleeing Ukraine, the information about the mass threat they posed was untrue. The police have repeatedly emphasized that there has been no increase in crime in the Przemyśl district and in the Podkarpackie region and at border crossings in Podkarpackie.

The disinformation narrative was prepared professionally, in accordance with the latest methods used by the Kremlin. Today, Russia is manipulating the society with false information that is not easy to verify. More often than not, it exaggerates the significance of individual real incidents, creates a false picture of the whole from random photos or recordings, and provides selective data without full context. This is exactly how the narrative about the threat posed by refugees from Africa and Asia was built. At the same time, it must be remembered that if this narrative had not fallen on fertile ground, it would have no meaning, like several other narratives that Russia has already tried to introduce into the information circulation during this war and has not been successful.

3 MANIPULATION OF AIR INCIDENTS (2022-2025)

Another manifestation of disinformation was the false message regarding drone attacks in Poland on September 10, 2025. Despite the fact that the consequences of a drone attack have not been revealed in the Podkarpackie Voivodeship so far, the Podkarpackie Voivodeship has also been subjected to fake news. Through disinformation in the Podkarpacie region, fake news was aimed at causing fear and a sense of danger among the inhabitants of the region. One of the elements of the narrative was to suggest that the targets of the strikes could have been the airport in Rzeszów and other infrastructure facilities in the Podkarpackie region (Lubera, 2025).

Another message spread was the claim that Ukraine was behind the attacks to "drag Poland into the war", which further fueled social fear (Radio Eska, 2025). At the same time, narratives relativizing the threat were used – e.g. claims that "nothing happened" or that the incidents were only "media theater", which was supposed to undermine trust in the authorities, the police and special services (Ministerstwo Cyfryzacji, 2025).

False visual materials were also used to build an atmosphere of danger – manipulated maps and graphics that indicated the alleged places where the drones fell in Podkarpacie. The analyses also showed that a significant proportion of comments on the Internet (about 60%) duplicated Russian narratives, which artificially increased the impression of widespread fear (BiznesAlert, 2025). The effect of such actions was an escalation of the sense of threat, weakening trust in public institutions and making it more difficult to verify true information in social media (Lubera, 2025).

Among the many examples of disinformation in Podkarpacie, the leading claims were:

1. The claim that "the airport in Rzeszów is the target" — messages suggesting an imminent local threat. Pro-Kremlin news channels, social media and some Russian media published insinuations and maps suggesting that the target of the attacks was to be, for example, the airport in Rzeszów or the infrastructure in Podkarpacie — this is a simple way to cause local panic.
2. The narrative "it is a provocation of Ukraine" — attributing responsibility to the party that would "drag us into the war." The theses repeated on Telegram and pro-Russian accounts that it was allegedly the Ukrainians who deliberately directed drones at Poland to provoke a conflict reduced the sense of security and strengthened social fear.
3. Relativizing and denying ("nothing happened", "it's a theatre") — fueling uncertainty and anger. Messages saying that the incident is a media provocation, or that the government is hiding the truth undermine trust in institutions and create a sense of danger, because people do not know who to believe. Official government warnings and analyses indicate that such narratives were deliberately disseminated.
4. Fake or manipulated photos/videos and maps - "visual evidence" that causes panic. Publishing manipulated maps or fabricated videos/photos suggesting destruction or flights over specific towns (e.g. location of airdrops over Podkarpacie), even if not real, causes emotions and the news spreads quickly on networks.
5. Mass comments and bots - increasing the impression that the threat is prevalent. Analyses show that a significant proportion (e.g. about 60%) of comments online about drone incidents reflected the Russian narrative, which intensifies the sense of widespread threat.

All examples of disinformation were clearly targeted, in particular:

1. causing anxiety among the inhabitants of the region (fear of further "attacks", concerns about the safety of flights and infrastructure),
2. erosion of trust in local authorities and services – when people see conflicting information, frustration and fear grow,
3. information chaos in social media, making it difficult to reach reliable messages,
4. causing reluctance to continue military and humanitarian aid to Ukraine.
5. Pro-Kremlin narratives have been amplified by bots and anonymous accounts, as well as by radical local groups. Fact-checker monitoring shows that the reach of this type of content has grown rapidly thanks to local discussion groups on Facebook and instant messaging.

4 HISTORICAL AND ANTI-UKRAINIAN DISINFORMATION IN THE CONTEXT OF PODKARPACIE (2022-2025)

Historical disinformation, especially referring to traumatic events, is one of the tools used by Russia to fuel social and international conflicts. In Polish-Ukrainian relations, the key thread is the memory of the Volhynian Massacre, the activities of the UPA and the ideology of Stepan Bandera.

Since 2022, Russian information campaigns in Poland, including Podkarpacie – a region bordering Ukraine – have increasingly begun to use the topic of the "Volhynian Massacre" to provoke Poles resentment towards Ukrainians. However, this disinformation is not limited to historical issues – it is also aimed at weakening support for humanitarian and military aid provided to Ukraine in the face of Russia's aggression.

Historical disinformation narratives:

"Echoes of Volhynia" - a fake document about the suspension of exhumations. A fabricated document allegedly issued by the Minister of Culture of Ukraine appeared on the Internet, which was supposed to order the suspension of the exhumation in Puźniki – the site of the crime against Poles in February 1945. The fake news was intended to create the belief that Ukraine does not respect the memory of the victims and consciously blocks historical reconciliation (TV Republika, 2025).

A narrative about "nationalism and Nazism". Russian propaganda sources presented Ukrainians as heirs to Nazi ideology, emphasizing the symbolism of the UPA and Stepan Bandera. This message was supposed to generalize historical guilt and build the image of Ukraine as a "fascist state" (Disinfo Digest, 2023).

Local incidents as a pretext for historical associations – after a bank robbery in Przemyśl in 2022, the perpetrator of which turned out to be a person with Russian-Ukrainian citizenship, comments appeared en masse online linking this case with banderism and stereotypes about Ukrainians as "savages" or "heirs of the UPA" (Marszałek, 2023).

5 DISINFORMATION NARRATIVES AGAINST AID TO UKRAINE

"Poles are suffering because of Ukrainians" - messages were spread suggesting that the influx of Ukrainian refugees allegedly deprives Poles of jobs, housing and social benefits. Such narratives were intended to arouse resentment and discourage further solidarity with Ukraine (Fundacja Geremka, 2025).

"Military aid weakens the Polish army" - one of the recurring threads was the narrative that the transfer of military equipment to Ukraine leads to the "disarmament of Polish" and puts Podkarpackie in danger. In this context, information about the presence of NATO troops in Rzeszów and the surrounding area was manipulated (EUvsDisinfo, 2023).

"Ukrainians ungrateful to Polish" - Russian disinformation channels promoted the thesis that despite the huge support from Poland, Ukrainians allegedly show a lack of gratitude and even harbor anti-Polish sentiments. The theme of Volhynian exhumations was also used here – the alleged blocking of the search for victims was supposed to prove Ukraine's "hostility" towards Poles.

"Escalation of the war" - theses were spread that providing military support to Ukraine "draws Poland into the war" and makes Podkarpacie a potential target for Russian drone or missile attacks. It was a narrative intended to instill fear in the border region.

Undoubtedly, disinformation activities have a strictly defined purpose, form and mechanism of action. The most common mechanisms include:

1. combining historical and contemporary threads – e.g. suggesting that the "Banderites from Volhynia" are the same ones who allegedly threaten Poles today,
2. polarization through emotional narratives – e.g. juxtaposing images of Volhynia victims with information about military assistance,
3. manipulation of the local context – taking advantage of the fact that Podkarpacie is the main hub of military and humanitarian aid (m.in. the airport in Jasionka),
4. undermining trust in institutions – suggesting that the government is hiding the costs of support for Ukraine or "exposing Poles to foreigners".

Analyzing the above, it is impossible not to notice that Russian disinformation in Podkarpacie in 2022–2025 is based on the synergy of two threads:

- historical (Volhynia, UPA, Bandera),
- contemporary (humanitarian aid for Ukraine).

Both of these threads are intertwined in order to provoke resentment towards Ukrainians, discourage Poles from providing military and humanitarian support, as well as building a sense of threat in the border region. For this purpose, various disinformation methods are used, which in the long term may cause an increase in social tensions in border cities, especially in Przemyśl.

The effectiveness of the "Kremlin" disinformation depended not so much on the quality of the materials as on the emotional charge of the message and distribution through local communication channels.

6 RECOMMENDATIONS FOR STRENGTHENING THE INFORMATION RESILIENCE OF THE REGION

1. Strengthening the crisis communication infrastructure.

Podkarpacie requires a developed network of fast communication between state institutions, local governments and regional media. The experience of the drone incident in September 2025 has shown that delays in official messages or the transmission of unverified, inaccurate messages are conducive to the spread of disinformation. The introduction of permanent crisis response protocols would allow to minimize this problem.

2. Media and digital education

A key element of building information resilience is the development of citizens' competences in recognizing manipulation and fake news. Research indicates that local communities with a high level of media education are less susceptible to propaganda. In Podkarpacie, it is worth introducing educational programs in schools and training for seniors, who are often particularly exposed to manipulation in social media.

3. Support for independent and local media

Disinformation is particularly rampant where there is a deficit of reliable sources of information. Therefore, it is important to support local newsrooms and investigative journalism through grants, partnership programs with universities, and content proofing training. The presence of strong regional media can serve as a "first line of defense" against fake news.

4. Cross-border cooperation

Podkarpacie, bordering Ukraine and Slovakia, should develop mechanisms for information cooperation with foreign partners. Coordinating disinformation monitoring activities and exchanging good practices (e.g. with Ukraine, which has been gathering experience in countering Russian propaganda since 2014) can significantly strengthen the region's resilience.

5. Activating civil society

NGOs, parishes, local associations and universities of the third age can act as natural "sensors" of disinformation. Involving them in the process of monitoring the media space and organizing fact-checking workshops increases the chances of quickly identifying and neutralizing false narratives.

6. Building social trust

Ultimately, the effectiveness of the fight against disinformation depends on the level of trust citizens have in public institutions. The lack of transparency and inconsistency in the actions of the state are conducive to vulnerability to fake news. Therefore, it is necessary for the authorities to have a transparent information policy and to involve residents in the decision-making process regarding local security.

CONCLUSION

The analysis of Russian disinformation in the Podkarpackie Voivodeship confirmed the correctness of the research hypothesis. The main hypothesis about the high degree of adaptation of Russian disinformation activities to the local conditions of Podkarpacie has been fully confirmed. The Russian Federation's propaganda campaigns demonstrate a sophisticated use of specific regional elements: the historical memory associated with the Volhynia Massacre, its strategic location as a NATO logistics hub, and local social sensitivities related to the influx of refugees.

Disinformation campaigns effectively exploit local historical and social conditions. The Podkarpackie region, due to its historical memory associated with difficult Polish-Ukrainian relations, is becoming particularly susceptible to narratives that refer to resentment and grievance. Russian propaganda instrumentalizes events from the past in order to cause distrust towards the contemporary actions of the Polish state and international alliances (Kojzar, 2022). Crisis incidents – such as the drone attack of September 9-10, 2025 – act as a catalyst that immediately triggers waves of false narratives (Charlish, Kelly, Erling, 2025). This mechanism is characteristic of modern information warfare: every sudden, not fully explained fact becomes a space for manipulation (The Guardian, 2025). The speed of the spread of fake news often outpaces the reactions of state institutions, which deepens the information chaos.

At the same time, the effect of Russian disinformation is not only the polarisation of public opinion, but also the erosion of trust in state and international institutions (e.g. NATO). In Podkarpacie, it can be observed that residents, bombarded with contradictory messages, are more likely to seek information from local, unverified sources or social media, which is conducive to the further spread of disinformation.

It is also important that every disinformation has real practical consequences. These include: the burden on security and law enforcement services, the need to conduct educational and fact-checking activities, as well as obstacles to humanitarian and local government activities (Kojzar, 2025). In crisis situations, such as a drone attack, administrative resources must be directed not only to security activities, but also to combat rumors.

The analysed narratives - from manipulation of air incidents, through the exploitation of the difficult Polish-Ukrainian past, to anti-immigration fake news - show that Russia is conducting propaganda activities with a high degree of adaptation to local conditions. Podkarpacie, as a border region, NATO's logistical base and the main humanitarian aid corridor, has become the target of particularly intense disinformation operations.

The conclusions of the conducted considerations indicate that disinformation not only polarizes society, but also undermines trust in state and international institutions. The most dangerous are crisis situations, such as the drone incident of September 2025, when the speed of spread of false content exceeds the pace of official communication.

The proposed recommendations allow us to outline a practical path to strengthen the information resilience of the region. It should be emphasized that effective defence cannot be understood only in military or technological terms, but as a socio-institutional process in which state authorities, local governments, the media, non-governmental organisations and citizens themselves cooperate. Media education, transparent crisis communication, support for independent media and the development of cross-border cooperation are the foundation on which to build sustainable information resilience.

To sum up, Russian disinformation in the Podkarpackie Voivodeship reveals the mechanisms of modern hybrid warfare, in which the line between military and information conflict is blurred. Due to its geographical location, "historical sensitivity" and multiculturalism, the Podkarpackie region is a kind of "laboratory" for researchers and practitioners of information security, showing that effective defense against manipulation requires the cooperation of state institutions, the media and citizens.

The conclusions from this region can be a valuable source of knowledge for the whole country and a reference point for security policies in Central and Eastern Europe.

REFERENCES

BEDNAREK, A. Uchodźcy w Przemyślu gwałcą kobiety to fake news ruskich trolli, publikacja 02.03.2022, SpidersWeb, DOI: https://spidersweb.pl/2022/03/uchodzcy-w-przemyslu-gwalca-kobiety-fake-news-ruskie-trolle-ruszyly-do-ataku.html [dostęp 22.09.2025].

BIZNESALERT, Rosyjska narracja dominuje o ataku dronów. Eksperci ostrzegają, publikacja 12 września 2025, DOI: https://biznesalert.pl/rosyjska-narracja-dominuje-o-ataku-dronow-eksperci-ostrzegaja/ [dostęp 25.09.2025].

CERT POLSKA, Raport roczny o incydentach cyberbezpieczeństwa, 2023, DOI: https://cert.pl/posts/2024/04/raport-roczny-2023/ [dostęp 25.09.2025].

CHARLISH, A. KELLY, L. ERLING, B. Poland downs drones in its airspace, becoming first NATO member to fire during war in Ukraine, publikacja 11.10.2025, Reuters, DOI: https://www.reuters.com/business/aerospace-defense/poland-downs-drones-its-airspace-becoming-first-nato-member-fire-during-war-2025-09-10/ [dostęp 25.09.2025].

DISINFO DIGEST, Operacje informacyjne Federacji Rosyjskiej i Republiki Białorusi w polskiej infosferze w lipcu 2023 roku, publikacja 10.08.2023, DOI: https://disinfodigest.pl/2023/08/10/operacje-informacyjne-federacji-rosyjskiej-i-republiki-bialorusi-w-polskiej-infosferze-w-lipcu-2023-roku/ [dostęp 25.09.2025].

EEAS, FIMI Report, 3 rd EEAS Report on Foreign Information Manipulation and Interference Threats), 2025r., DOI: https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf [dostęp 25.09.2025].

EUVFSDISINFO, Raport: Rosyjska dezinformacja wobec pomocy wojskowej dla Ukrainy, 2023, DOI: https://euvsdisinfo.eu/pl/wojna-nadal-trwa-rosyjska-dezinformacja-przeciwko-ukrainie/ [dostęp 25.09.2025].

FINANCIAL TIMES, Poland reports surge in Russian cyberattacks, 2024, DOI: https://www.ft.com/content/3e7c7a96-09e7-407f-98d7-a29310743d28 [dostęp 25.09.2025].

FUNDACJA GEREMKA, Raport. Przeciwdziałanie dezinformacji. O uchodźcach wojennych z Ukrainy w Polsce i wzrostowi nastrojów anty-ukraińskich w Polsce, 2025, DOI: Fhttps://geremek.pl/wp-content/uploads/2025/08/PrzeciwdzialaniedezinformacjiouchodzcachwojennychzUkrainywPolsceraportzmonitoringukwiecienlipiec225.pdf [dostęp 25.09.2025].

JONES, S. G. Russia's Shadow War Against the West, Center For Strategic & Internal Studies (CSIS), 2024, DOI: https://www.csis.org/analysis/russias-shadow-war-against-west [dostęp 25.09.2025].

KANCELARIA PREZESA RADY MINISTRÓW, Zespół ds. dezinformacji, Raporty o stanie bezpieczeństwa informacyjnego Polski, Warszawa 2023, DOI: https://share.google/j2tBZmihNg5DNPyJF [dostęp 25.09.2025].

KOJZAR, K. Kłamstwa o uchodźcach zalewają Przemyśl. Policja prostuje fake newsy, publikacja 02.03.2022, OKO.press, DOI: https://oko.press/dezinformacja-zalewa-przemysl-policja-to-przekazy-ktore-maja-wystraszyc-mieszkancow-i-uchodzcow [dostęp 25.09.2025].

LUBERA, J. Rosyjska propaganda ruszyła. Twierdząc, że Polska nie ma dowodów i publikują fałszywe mapy, Radio Eska, publikacja 10 września 2025, DOI: https://www.eska.pl/wiadomosci/rosyjska-propaganda-ruszyla-twierdza-ze-polska-nie-ma-dowodow-i-publikuja-falszywe-mapy-aa-4XyP-uPj4-8n7B.html [dostęp 25.09.2025].

MARSZAŁEK, M. Wojna i rosyjska dezinformacja. Jakie trendy przyniósł ostatni rok, publikacja 23.02.2023, „Demagog", DOI: https://demagog.org.pl/analizy_i_raporty/wojna-i-rosyjska-dezinformacja-jakie-trendy-przyniosl-ostatni-rok/ [dostęp 22.09.2025].

MENKISZAK, M. Rosyjska dezinformacja wobec Polski w kontekście wojny na Ukrainie, Ośrodek Studiów Wschodnich, Warszawa 2022, DOI: https://www.osw.waw.pl/sites/default/files/PW_91_Urwa%C4%87-%C5%82eb-hydrze.pdf [dostęp 25.09.2025].

MIERZYŃSKA, A. Rasistowskie ataki w Przemyślu. Jak udało się doprowadzić do „polowania na ludzi'?, „Gazeta Wyborcza", publikacja 04.03.2022, wyborcza.pl., DOI: https://wyborcza.pl/7,162657,28184979,jak-zorganizowac-polowanie-na-ludzi-wystarczy-internet-i-trafiony.html [dostęp 22.09.2025].

MINISTERSTWO CYFRYZACJI, Uwaga na dezinformację związaną z naruszeniem polskiej przestrzeni powietrznej przez drony, publikacja 11 września 2025, gov.pl,. DOI: https://www.gov.pl/web/cyfryzacja/uwaga-na-dezinformacje-zwiazana-z-naruszeniem-polskiej-przestrzeni-powietrznej-przez-drony [dostęp 22.09.2025].

NATO StratCom COE, Hybrid Threat Trends, 2024, https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf (dostęp 25.09.2025).

RADIO ESKA, Rosyjska dezinformacja po incydencie z dronami. Minister Krzysztof Gawłowski ujawnia szczegóły, publikacja 11 września 2025.

THE GUARDIAN, Poland dismisses Russia's claim drone incursion was unintentional, publikacja 10.09.2025, DOI: https://www.theguardian.com/world/live/2025/sep/10/poland-pm-condemns-repeated-violation-of-airspace-amid-russian-attack-on-ukraine-follow-live [dostęp 25.09.2025].

TV REPUBLIKA, Echa Wołynia w ogniu rosyjskiej propagandy, publikacja 07.06.2025, DOI: https://tvrepublika.pl/Polityka/Echa-Wolynia-w-ogniu-rosyjskiej-propagandy/190630 [dostęp 22.09.2025].

ret. col. Piotr ZALEWSKI, Ph.D.
Jan Kochanowski University of Kielce,
ul. Uniwersytecka 15
25-406 Kielce
Telefon: +48 41 349 65 25
e-mail: piotr.zalewski@ujk.edu.pl

podinsp. Janusz KISZKA, Ph.D.
State Univesrity of Applied Sciences in Przemyśl
ul. Książąt Lubomirskich 6
37-700 Przemyśl
Telefon: +48 16 7355 100
e-mail: janusz19051977@interia.pl

DOI: https://doi.org/10.52651/vr.a.2025.3.31-44
VOJENSKÉ REFLEXIE
ISSN: 1336-9202 (online)
2025, Number 3, Page 31-44

SLOVAKIA AS A TARGET OF RUSSIAN DISINFORMATION CAMPAIGNS

Jakub NYÉKI

ARTICLE HISTORY

Submitted: *28.10.2025*
Accepted: *27.11.2025*
Published: *31.12.2025*

ABSTRACT

The phenomenon of hybrid warfare has become an inherent part of our daily lives, and the dissemination of disinformation is its vital component.
A notable increase in the dissemination of disinformation within the information space has been observed since the Russian annexation of Crimea in 2014. To pursue its objectives, the Russian Federation is influencing the development in other countries through non-conventional means, and the dissemination of disinformation is one of the many tools in its arsenal. It is unfortunate, but Slovakia is not an exception to this rule. In this study, the author employs a dual approach, integrating qualitative and quantitative methodologies, to assess Slovakia's vulnerability to disinformation. The paper will provide a detailed analysis of the various factors and particularities of Slovak society that contribute to its vulnerability. The subsequent examination will address the methods and means by which disinformation is disseminated into Slovakia's information space, and the manner in which it is disseminated within the population. The objective of conducting this analysis is to enhance our comprehension of the underlying causes of the problem and to identify potential solutions.

KEYWORDS

Hybrid warfare, disinformation, Russian Federation, information warfare, alternative media

INTRODUCTION

In recent years, we have witnessed growing tensions between the Russian Federation and NATO. It is important for Russia to undermine the cohesion of NATO member states and their internal stability as much as possible, in order to weaken the overall cohesion and response capacity of the alliance in the event of an open conflict. Hybrid warfare is the primary tool used by the Russian Federation in times of "peace" to achieve this goal. Within the framework of hybrid operations, disinformation is most often used to influence the public opinion of the opponent with the aim of dividing society, sow uncertainty, arouse insecurity, and question democratic principles, undermining its cohesion and thus reducing the overall defence capability of the opponent. The Slovak Republic is undoubtedly a frequent target of Russian disinformation campaigns due to its sensitive location on the eastern flank of NATO. Based on the experience of the last presidential and parliamentary elections, when society was extremely divided, we can conclude that these disinformation campaigns were successful in Slovakia. Based on the GLOBSEC (2025), 43% of the Slovaks believe that "Democracy does not exist, because in reality, hidden elites rule the world" and 46% believe that "World affairs are not decided by elected leaders but by secret groups aiming to establish a totalitarian world order". We will try to find out why Slovakia is so susceptible to disinformation. In the opening chapter, a comprehensive definition of pivotal terminology is provided, with particular emphasis on the comprehension of these concepts within the paradigm of hybrid warfare. In the subsequent chapter, an examination will be conducted of the key factors that render Slovakia vulnerable to Russian disinformation campaigns. Finally, the focus will be on the methods employed by the Russian Federation to conduct disinformation campaigns in the Slovak information space.

METHODOLOGY

This study uses a combination of qualitative and quantitative scientific research. Its aim is, firstly, to understand the nature of the spread of disinformation, its scope and its impact on the public; and secondly, to identify the factors that influence the dissemination of disinformation within the Slovak information space.

The qualitative element of the research uses content analysis and discursive analysis, which facilitate an examination of the factors contributing to the widespread success of pro-Russian narratives in Slovakia. In this context, the author aims to examine the manner in which narratives are adapted to the Slovak audience, with a particular focus on the utilisation of historical contexts, the escalation of political polarisation, and the augmentation of pro-Russian sentiments within Slovak society.

The quantitative element of the study lends support to the findings of the qualitative research through indicators of the spread of disinformation in Slovakia and by analysing the repetition of disinformation narratives. The statistical analysis of this data facilitates the identification of prevalent narratives within the Slovak information space and the subsequent analysis of the online platforms utilized for their dissemination.

1 DEFINITION OF KEY TERMS

To ensure a clear understanding of the topic and its broader context, it is essential to first define the fundamental terms used in this study that need to be understood correctly.

Terms such as disinformation, hybrid warfare, information warfare, and alternative media are frequently used in both academic and public discourse, but their meanings may often vary depending on the context they are used in. This can cause conceptual ambiguity that can lead to inconsistencies or inaccurate interpretations.

The following definitions, therefore, provide important theoretical definitions of these key terms, based on relevant scholarly sources. The aim is to establish a coherent framework that will serve as the basis for their further understanding of the topic analysed in this paper.

1.1 Disinformation

Unfortunately, disinformation is part of our daily lives, and its quantity and quality are growing exponentially. Disinformation often undermines trust in institutions, digital and traditional media, and damages democracies by preventing citizens from making informed decisions. Disinformation also often promotes radical and extremist ideas, activities, or narratives spread by the party that has an interest in it. The European Commission defines disinformation as *"as verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm".* (European Commission, 2018, p. 3-4)

Disinformation is an ever-evolving threat that requires continuous efforts to identify relevant actors, tools, methods, priority targets, and impact. Some forms of disinformation, particularly the one spread and commissioned by states, are particularly dangerous. However, disinformation can also be spread by non-state actors and even by individuals within a state. (Ivančík, 2025a)

NATO, for example, regards disinformation *"as the deliberate creation and dissemination of false and/or manipulated information with the intent to deceive and/or mislead. Disinformation seeks to deepen divisions within and between Allied nations, and to undermine people's confidence in elected governments."* (NATO, 2020)

Disinformation is an integral part of information, psychological, intelligence, and cyber operations, which form the core of hybrid threats. (Ivančík, 2025b) Disinformation as part of hybrid threats is part of the broader concept of hybrid influence and hybrid actions that aim to disrupt and destabilize the target society through various tactics, methods, and means. (Ivančík, 2025a)

According to Jurčák (2018), hybrid warfare is a combination of activities (actions) of a military and non-military nature, carried out by state and non-state actors, or interest groups, which work in synergy and organize their activities at the same time and with the same goal, whereby their goal is to destabilize, neutralize, or degrade the reference object.

1.2 Hybrid warfare

A particular change in the perception of hybrid warfare occurred after the annexation of Crimea in 2014, when the number of publications on this issue increased exponentially. The concept of hybrid warfare began to be directly associated with the activities of the Russian Federation. Many authors and institutions began to address this issue on a larger scale and also attempted to define the term. (Andrassy, Ondruš, 2024)

Hybrid warfare is a type of armed conflict in which both conventional and unconventional methods of combat are used. Hybrid warfare combines various tools, including not only traditional military, political, and economic ones, but also cyber and information tools, with the primary goal of weakening the enemy's internal stability. *“Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace and attempt to sow doubt in the minds of target populations. They aim to destabilise and undermine societies”*. (NATO, 2024)

Hybrid warfare can be understood as a broad spectrum of hostile activities in which the military component is rather small, because political, informational, economic, and psychological influence becomes the main means of waging war. Such methods help to achieve significant results: territorial, political, and economic losses for the enemy, chaos and disruption of the system of state power, and a weakening of society's morale. (Manko, Mikhieiev, 2018)

The Slovak national security bureau defines hybrid warfare as a set of coercive and subversive activities, conventional and unconventional, military and non-military methods, which can be used by state and non-state actors in a coordinated manner to achieve specific goals without a formal declaration of war below the threshold of a normal response. (NBÚ, n.d.)

Within the context of the Slovak Republic, hybrid warfare can be conceptualised as a component of a broader security threat, wherein information operations and disinformation campaigns serve as effective instruments for foreign actors to influence public opinion and impact domestic political processes.

1.3 Information warfare

The positive impact on the population resulting from technological progress is sometimes accompanied by negative effects. This is also true in the case of information dissemination. Historically, warfare only took place in traditional domains such as land, air, and sea. Nowadays, battles are also fought in cyberspace, in space, and in the information space. Information warfare enables actors in the international arena to enforce their interests without the use of force. Information warfare can also be implemented where traditional military force cannot be used, either for legitimacy reasons or in an effort to conceal an actor´s intentions. Information can also be used in the preparation of the operational environment prior to the use of conventional warfare. NATO (n. d.) defines information warfare as *“an* *operation conducted in order to gain an information advantage over the opponent. It consists in controlling one's own information space, protecting access to one's own information, while acquiring and using the opponent's information, destroying their information systems and disrupting the information flow. Information warfare is not a new phenomenon, yet it contains innovative elements as the effect of technological development, which results in information being disseminated faster and on a larger scale."*

According to van Vuuren (2016) *"Information warfare is defined as actions focused on destabilising or manipulating the core information networks of a state or entity in society with the aim to influence the ability and will to project power as well as efforts to counter similar attacks by an opposing entity and/or state."* These definitions make it clear that decision-makers and military planners must also pay close attention to this area in their efforts to ensure the sovereignty of the country.

1.4 Alternative media

The term 'alternative media' is used to denote media entities that present themselves as opposition to the so-called mainstream or traditional media. From an academic perspective, alternative media comprise a broad spectrum of actors, ranging from civic initiatives and independent journalism projects to websites and platforms that systematically disseminate manipulative or disinformation content. The common features of such publications tend to be a lack of editorial standards, unclear ownership structures, insufficient verification of information, and strong bias.

John Carroll University (2023) defines alternative media as *"media sources that differ from established or dominant types of media (such as mainstream media or mass media) in terms of their content, production, or distribution. Sometimes the term independent media is used as a synonym, indicating independence from large media corporations, but generally independent media is used to describe a different meaning around freedom of the press and independence from government control. Alternative media does not refer to a specific format and may be inclusive of print, audio, film/video, online/digital and street art, among others."*

According to other scholars, alternative media are understood in relational terms, positioning themselves as corrective forces that stand in opposition to mainstream news discourses. They suggest that such media function as critical observers and challengers of dominant narratives, offering counter-perspectives within the broader media environment. In this conceptualization, the notion of "alternative" stems not from structural or formal differences, but from the stance of opposition such media adopt toward established journalism. (Ihlebæk et al., 2022)

In his work, Kapas (2018) elaborates on the issue of alternative media and compares them with mainstream media, defining them as follows:

- they disseminate information that is not covered by mainstream media at all, or not to the full extent,
- they are often, but not exclusively, created by non-professionals,
- hey are characterized by the dissemination of unverified information, alarmist reports, misinformation, and conspiracy theories,
- differ from the mainstream in their artistic output through a more demanding form of production or reception,
- in times of technological progress, they represent an alternative in the form of technical improvement or a completely new way of producing, distributing, or receiving media expressions.

Based on all the definitions mentioned above, we can judge that the term “alternative media” should not be understood in a negative point of view. The idea of alternative media is not malign in its nature, but it is very often abused.

2 SLOVAKIA IN THE CONTEXT OF HYBRID WARFARE

Each country has its own specific characteristics and unique features that shape its fundamental direction and values. These factors also influence a country's overall defence capabilities as well as its resilience. This is also true in the case of the Slovak Republic and its ability to defend itself against disinformation and hybrid warfare. In this chapter, we will therefore examine the factors that make Slovakia vulnerable to disinformation campaigns by the Russian Federation.

2.1 Ethnic and historical aspects

There are many reasons why Slovakia is a good target for Russian disinformation campaigns. From the ethnic point of view, the definitive majority of the population of Slovakia are Slavs. Therefore, many Slovaks tend to lean towards Russia as “they are the same people as we are and who share the same values as we do”.

According to the Russian Federation´s propaganda, there are plenty of historical reasons why Slovaks should incline to Russia:

- Slavic, pro-Russian sentiment of the historical Slovak national movement,
- liberation from the Nazi occupation by the Red Army in the Second World War,
- 40 years of “prosperity” under the communist regime (bolstered by the nostalgic optimism of a part of the older generation),
- decline in living standards after the Velvet Revolution and uncertainty associated with the introduction of a new political system and social order in the 1990s. (Šmihula, 2024)

Some may argue that the evidence of Russian aggression in Ukraine and attacks on defenceless civilians should convince those who feel sympathy for Russia that Russia is an aggressor and a real threat. But there are other psychological factors e.g., cognitive dissonance that influence general perception of the population. Cognitive dissonance is a state in which there is a difference between your experiences (Russia acts aggressively) and your beliefs about what is true (Russia is not a threat). (Cambridge University Press, n. d.) However, people experiencing cognitive dissonance crave to maintain their original stance. They believe misinformation and propaganda regardless of how absurd it is because it allows them to support their beliefs. Thus, disinformation is successful not because it is a sophisticated or intellectually elaborate argument, but because targeted individuals do not have to think of Russia as an aggressor. It allows them to resolve the discomfort they experience in their opinions. (Jarcho et al., 2011) All these points provide a good basis for the production of Russian propaganda.

2.2 Political polarization

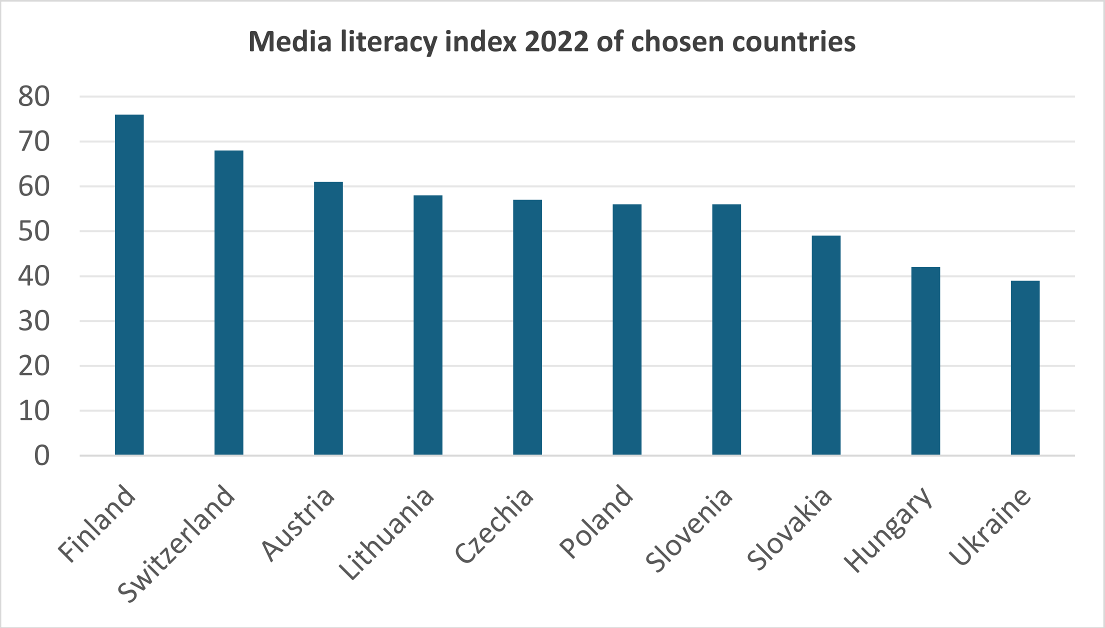
The Slovak political environment is currently based on very high polarization. The division between the left and right is reaching extreme and unusual levels. During the last presidential and parliamentary elections in 2024 and 2023, respectively, the main topics of the political debates and political campaigns were very emotional, divisive, and binary. The aggressive verbal expressions of politicians only added fuel to the fire in an already very tense social situation. It is very easy to spread disinformation in these conditions because if they support the argument of one or the other group, they are spread at tremendous speed as the opinion becomes part of the people's personality, and in their point of view, it needs to be defended and supported. War in Ukraine, migration, discourse on gender and sexual diversity, and vaccination became the main talking points. On these topics, it is required to adhere to only one opinion or the other, there is no compromise. This caused even greater polarization of the already divided population. Other, and one can say more important topics like pension system, aging population, healthcare (accessibility, quality, funding), education reform and modernization, family policy, and social welfare were pushed to the periphery of the public interest due to their low emotional impact.

2.3 Cognitive factors

One of the potential reasons why Slovakia is vulnerable to disinformation might be the lack of innate cognitive abilities. But according to the Lynn & Becker study (2019), the average IQ of a Slovak population is 96 points, which results in an approximate ranking of 33rd to 39th in the world. This is a rather neutral ranking in relation to susceptibility to disinformation.

Critical thinking is very closely connected with creative thinking. Based on the PISA 2022 study, the Slovak Republic achieved a score of 29 points in creative thinking, while the average was 33 points. (OECD, 2023) According to the latest surveys among primary school teachers, although up to 96% of respondents consider the development of critical thinking to be important, only 17% said they use methods to develop it regularly. Most perceive the need for greater systemic support and better tools to develop these skills. More than half of teachers would welcome the introduction of a separate subject devoted to critical thinking, but a large proportion prefer an integrated approach within regular subjects without increasing teaching hours. According to 38% of teachers, the biggest barriers to the development of critical thinking are a lack of methodological materials, and according to 28%, their concern is that they will not have time to cover all the necessary material. (Rapčan, Štrompová et al., 2025) It is very worrying that even teachers themselves feel that critical thinking is not given sufficient attention in the educational process. The result is a society that lacks developed critical thinking skills, which makes it more susceptible to disinformation campaigns.

The research on media literacy index assesses the potential vulnerability of 41 European societies to the so-called "fake news" and related phenomena by employing indicators of media freedom, education, and interpersonal trust. The research includes the EU member states, the EU candidate and potential candidate countries, prospective candidates, the countries in closer relations with the EU, such as the European Economic Area (EEA) and Switzerland as well, as the UK. In this study, Slovakia once again ranked below average, in 24th place. (OSCE, 2022)



Graph 1 Media literacy index 2022 of chosen countries

Source: OSCE, 2022

Although the population in Slovakia has good genetic intelligence predispositions in terms of intelligence, it is still very vulnerable to the spread of disinformation. This is mainly due to the insufficient development of critical thinking within the country's education system. Furthermore, resistance to disinformation from Russia is also influenced by historical and ethnic factors, which have a particularly strong impact on the older generation, who experienced a totalitarian regime in which they were also educated.

2.4 Tools of disinformation dissemination

The first significant increase in the spread of disinformation in Slovakia was recorded after Russia's annexation of Crimea in 2014, as it became an integral part of the Russian Federation's operations. The amount of disinformation spread remained stable until Russia invaded Ukraine in 2022, when it was increased again. With the conventional invasion underway, unconventional operations also began, and the spreading of disinformation is a vital part of it.

Social networks are clearly effective in spreading disinformation and are therefore the most common place where such misinformation is disseminated. More traditional media such as television and online newspapers lag behind, but they still clearly play a role. We saw the first significant increase in the spread of disinformation at the onset of the COVID-19 pandemic, as a lack of information and uncertainty left a large information vacuum that was exploited by disinformers. After the war in Ukraine began, most of the users, websites, and portals that had spread disinformation in connection with the pandemic began to spread disinformation about the war while they kept their audience.

One of the reasons why information and misinformation spread through social networks and why alternative media remain so popular is the existence of echo chambers phenomenon and confirmation bias. Confirmation bias is *"seeking or interpreting of evidence in ways that are partial to existing beliefs, expectations, or a hypothesis in hand"* (Nickerson, 1998, p. 175). An echo chamber is defined as *"a network of users in which users only interact with opinions that support their pre-existing beliefs and opinions, and they exclude and discredit other viewpoints"* (Alatawi et al., 2021, p. 1).

There are many popular social networks in Slovakia, and the most popular ones are undoubtedly Facebook, Instagram, X, TikTok, and Telegram. Although Telegram is not the most popular one, it plays a very important role in spreading Russian disinformation.

Telegram channels allow individuals or organizations to publish content—text statuses, videos, or photos—in the same way we are used to, for example, from Facebook wall. The advantage of Telegram channels is that users have subscribed channels listed among their regular chat conversations. When a channel publishes new content, it moves to the top of the list of unread conversations for subscribers, who can also opt to receive push notifications. This, together with the ability for subscribers to share content further, allows Telegram posts to reach tens of thousands of views. Users can comment on individual posts, or the owner can link their channel to a separate discussion group for up to 200,000 users. (Príbelský, 2023)

The former chief of the Center for Combating Hybrid Threats at the Ministry of the Interior of the Slovak Republic Daniel Milo mentioned that Telegram´s importance is significant because, according to our internal analysis, up to 20% of the content on Slovak

Telegram channels and accounts is taken from Russian-language sources. These are 99.9% Russian propaganda and information operations. This content is then spread from Slovak Telegram groups and channels to Facebook, where it is shared by so-called "influencers." These influencers may be politicians or non-political actors. From there, the content is often spread further with the help of disinformation media outlets, which often simply repost Facebook statuses, especially those of politicians, and publish them as their own articles. (Hodás, Príbelský, 2023) Telegram is not particularly significant in Slovakia, with approximately 100,000 to 200,000 users. (Kőváry Sólymos and Šlerga, 2023) What makes it important is its role as a gateway for Russian narratives into the Slovak information space, as described above.

2.5 Other masmedias

Television and online magazines are a very important part of the Slovak information space. Unfortunately, frequent attacks from the politicians and other high-profile state representatives undermined public trust in traditional media outlets in Slovakia. According to the Digital News Report 2023, trust in news in Slovakia was among the lowest. This was caused by decades of interference by business and political leaders in the chase of their goals. In 2023, the overall trust in news in Slovakia is only 27% which ranks Slovakia 42nd out of the 46 countries covered. (Newman et al., 2023) This statistic is alarming in itself. What is even worse, however, is that people who do not trust traditional media mostly start consuming information elsewhere. Usually, this means the aforementioned social networks or alternative media.

The primary function of alternative media should be to facilitate public discourse by fostering a diversity of opinions. The credibility of alternative media is called into question when there is evidence to suggest that their primary objective is not the dissemination of factual information, but rather the deliberate propagation of false or manipulated content, with the ultimate aim of influencing public opinion. Furthermore, if such actors were to disseminate information with the objective of engendering instability within a specific nation for the benefit of a foreign power, they could potentially pose a significant threat. In Slovakia, the operation of alternative media commenced in 2014 on a larger scale, following Russia's annexation of Crimea, and these media outlets gained the greatest popularity after the onset of the COVID-19 pandemic.

The most popular alternative media outlets in Slovakia include *Zem a vek*, *infovojna.sk*, *Slovenské noviny*, and *Hlavné správy*. Alternative media are part of the information space that benefits from the existence of social networks such as Telegram and similar platforms. In their posts, they often cite unverified sources from social networks, or they share articles reciprocally between individual alternative media outlets. Through these practices, they create an illusion of credibility and "generally accepted validity" of the information they share. Based on the research done by Mintal et al. (2021), most of the untrustworthy media operating in the Slovak information space are based in Slovakia and not abroad. The research also shows that their primary goal is probably to generate profit, as they often display advertisements to a large extent. This contradicts the generally accepted view that these media outlets are sponsored from abroad. On the other hand, it does not refute it either, and if such sponsorship is carried out in a sophisticated manner, it may not be easy to detect without the use of sophisticated investigative methods and resources.

CONCLUSION

The Slovak Republic is influenced by various external and internal factors that make it susceptible to certain narratives that are part of a relatively successful disinformation campaign. These mainly concern historical and ethnic realities shared by Slovakia and the Russian Federation. Furthermore, there is already existing social polarization, which provides fertile ground for sowing further uncertainty and conflict between different social groups within the population. What´s more, the level of critical thinking and media literacy in Slovakia is below the European average. This poses a major challenge for the country, as it is caused by the insufficient integration of critical thinking into the education process for children. Remedying this situation may take several years, which means that Slovakia’s resilience will continue to suffer until then.

The Slovak information space has undergone major changes in the last decade. Traditional media have lost popularity, and this vacuum has been filled by newly emerging alternative media, which have experienced an extreme surge in popularity, especially during the COVID-19 pandemic. Another problem is that many people consider social networks to be a valid source of information, even though anyone can share anything on a social network without any proof. For this reason, social networks are very often used to infiltrate disinformation into the Slovak information space, where it is further disseminated as legitimate information.

All these factors contribute to a decline in the Slovak Republic's defensive capabilities, as disinformation is part of the Russian Federation's efforts to destabilize Slovakia and other the NATO or EU member states. Some of the factors mentioned can be improved more easily, while others are more complex. Similarly, improvements in some areas can be made more quickly than in others. For example, the introduction of a comprehensive mechanism for developing critical thinking for school-age children requires careful preparation, and the results of this process will only be seen later. However, such a change can have a positive and lasting impact on the country's future, as a change in this area can eliminate other negative influences (the amount of misinformation on social networks, the number of alternative media, the polarization of society) and improve overall defensive capabilities of the Slovak Republic.

REFERENCES

ALATAWI, F., CHENG, L., TAHIR, A., KARAMI, M., JIANG, B., BLACK, T. & LIU, H. (2021). 'A survey on echo chambers on social media: Description, detection and mitigation', *arXiv*. Available at: https://europepmc.org/article/PPR/PPR454066 (Accessed: 1 October 2025).

ANDRASSY, V. & ONDRUŠ, M. (2024). 'Pohľad na problematiku hybridnej vojny po anexii Krymského polostrova', *Vojenské reflexie*, 19(1), pp. 24–36. DOI: (Accessed: 14 October 2025). https://doi.org/10.52651/vr.j.2024.1

CAMBRIDGE UNIVERSITY PRESS (n.d.). *Cognitive dissonance*. *Cambridge Dictionary*. Available at: https://dictionary.cambridge.org/dictionary/english/cognitive-dissonance (Accessed: 2 October 2025).

EUROPEAN COMMISSION (2018). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions* (COM(2018) 236 final). Brussels: European Commission. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&rid=2 (Accessed: 8 October 2025).

GLOBSEC (2025). *GLOBSEC Trends 2025: Ready for a New Era?* Bratislava: GLOBSEC. Available at: https://www.globsec.org/sites/default/files/2025-05/GLOBSEC%20Trends%202025_1.pdf (Accessed: 28 September 2025).

HODÁS, M. & PRÍBELSKÝ, M. (2023). 'Slováci konzumujú ruskú propagandu „na milióny". Je im šitá na mieru (rozhovor)', *Živé*. Available at: https://zive.aktuality.sk/clanok/aHlrlwZ/slovaci-konzumuju-rusku-propagandu-na-miliony-je-im-sita-na-mieru-rozhovor/ (Accessed: 2 October 2025).

IHLEBÆK, K.A., et al. (2022). 'Understanding alternative news media and its contribution to diversity', *Digital Journalism*, 10(8), pp. 1267–1282. DOI: 10.1080/21670811.2022.2134165 (Accessed: 8 October 2025).

IVANČÍK, R. (2025a). *Dezinformácie. Teoretické východiská ich skúmania.* Praha: Leges. ISBN 978-80-7502-769-6.

IVANČÍK, R. – NEČAS, P. (2025b). *Hybridné hrozby: Bezpečnostná výzva pre demokratické spoločnosti.* Praha: Leges, 2025. 226 s. ISBN 978-80-7502-823-5.

JARCHO, J.M., BERKMAN, E.T. & LIEBERMAN, M.D. (2011). 'The neural basis of rationalization: Cognitive dissonance reduction during decision-making', *Social Cognitive and Affective Neuroscience*, 6(4), pp. 460–467. DOI: 10.1093/scan/nsq054 (Accessed: 29 September 2025).

JOHN CARROLL UNIVERSITY (2023). *Alternative Media Guide.* Available at: https://researchguides.jcu.edu/c.php?g=1422777 (Accessed: 14 October 2025).

JURČÁK, V. et al. (2018). *Identifikácia príznakov vedenia hybridnej vojny.* Liptovský Mikuláš: Akadémia ozbrojených síl generála M. R. Štefánika.

KAPEC, M. (2021). *Mainstreamové vs alternatívne médiá v slovenskom mediálnom priestore.* Trnava: University of St. Cyril and Methodius in Trnava. Available at:

https://www.ucm.sk/files/sk/ine-pracoviska/centrum-informacnych-zdrojov-ucm-trnave/referat-informacnych-sluzieb/e-zdroje/ucebne-texty-k-stiahnutiu/mainstreamove_vs_alternativne_media_v_slovenskom_medialnom_priestore.pdf (Accessed: 14 October 2025).

KŐVÁRY SÓLYMOS, K. & ŠLERGA, J. (2023). *Tok klamstiev: Telegram je priestorom neobmedzených možností pre dezinformácie a konšpirácie.* ICJK. Available at: https://www.icjk.sk/238/Tok-klamstiev-Telegram-je-priestorom-neobmedzenych-moznosti-pre-dezinformacie-a-konspiracie (Accessed: 1 October 2025).

LYNN, R. & BECKER, D. (2019). *The Intelligence of Nations.* London: Ulster Institute for Social Research. Available at: https://www.ulsterinstitute.org/ebook/THE%20INTELLIGENCE%20OF%20NATIONS%20-%20Richard%20Lynn,%20David%20Becker.pdf (Accessed: 30 September 2025).

MANKO, O. & MIKHIEIEV, Y. (2018). 'Defining the concept of "hybrid warfare" based on analysis of Russian aggression against Ukraine', *Information & Security: An International Journal*, 41, pp. 11–20. ISSN 0861-5160. https://doi.org/10.11610/isij.4107

MINTAL, J.M., KALMAN, M. & FABIÁN, K. (2021). 'Hide and seek in Slovakia: Utilizing tracking code data to uncover untrustworthy website networks', in *Multidisciplinary International Symposium on Disinformation in Open Online Media*, pp. 101–111. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-87031-7_7

NATO (n.d.). *Media – (Dis)information – Security: What is information warfare?* Available at: https://deepportal.hq.nato.int/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf (Accessed: 14 October 2025).

NATO (2024). *Countering hybrid threats.* Available at: https://www.nato.int/cps/en/natohq/topics_156338.htm (Accessed: 9 October 2025).

NATO (2025). *NATO's approach to countering disinformation: A focus on COVID-19.* Available at: https://www.nato.int/cps/en/natohq/177273.htm (Accessed: 6 October 2025).

NBÚ (n.d.). *Krátky slovník hybridných hrozieb.* Available at: https://www.nbu.gov.sk/kratky-slovnik-hybridnych-hrozieb/ (Accessed: 9 October 2025).

NEWMAN, N., FLETCHER, R., EDDY, K., ROBERTSON, C. & KLEIS NIELSEN, R. (2023). *Reuters Institute Digital News Report 2023.* DOI: 10.60625/risj-p6es-hb13 (Accessed: 30 September 2025).

NICKERSON, R.S. (1998). 'Confirmation bias: A ubiquitous phenomenon in many guises', *Review of General Psychology*, 2(2), pp. 175–220. https://doi.org/10.1037/1089-2680.2.2.175

OECD (2023. *PISA 2022 Results (Volume I): The state of learning and equity in education.* Paris: OECD Publishing. DOI: 10.1787/53f23881-en (Accessed: 30 September 2025).

OSCE (2022). *Media Literacy Index 2022: Main findings and possible implications.* Vienna: OSCE. Available at: https://www.osce.org/files/f/documents/0/4/534146.pdf (Accessed: 28 September 2025).

PRÍBELSKÝ, M. (2023). 'Neviditeľný nástroj vojny: Dezinformácie Slovákom šijú na mieru. Nie je to náhoda', *Aktuality.* Available at: https://www.aktuality.sk/clanok/wLVKPuc/neviditelny-nastroj-vojny-dezinformacie-slovakom-siju-na-mieru-nie-je-to-nahoda/ (Accessed: 30 September 2025).

RAPČAN ŠROMPOVÁ, A., NORISOVÁ, V. & MACKOVÁ, P. (2025). *Rozvoj kritického myslenia v mladšom školskom veku: Analýza výsledkov prieskumu medzi pedagogickými pracovníkmi a ich reflexia praxe.* Bratislava: Rada pre mediálne služby. Available at: https://www.rpms.sk/sites/default/files/2025-06/Prieskum_Rozvoj_kritickeho_myslenia_v_mladsom_skolskom_veku_2025.pdf (Accessed: 30 September 2025).

ŠMIHULA, D. (2024). 'Historické korene slovenskej rusofílie a jej dôsledky', *Denník N*. Available at: https://dennikn.sk/3915247/historicke-korene-slovenskej-rusofilie-a-jej-dosledky/ (Accessed: 25 September 2025).

VAN VUUREN, R. (2016). 'Information warfare', *Journal of Futures Studies*, 21(1), pp. 77–96. Available at: https://jfsdigital.org/wp-content/uploads/2018/10/06-Information-warfare-R-van-Vuuren.pdf (Accessed: 14 October 2025).

1LT Mgr. Jakub NYÉKI
external doctoral student
Department of Security and Defence
Armed Forces Academy of the General M. R. Štefánik
Telephone: +421 902 875 498
E-mail: jakub.nyeki@gmail.com

DOI: https://doi.org/10.52651/vr.a.2025.3.45-56

VOJENSKÉ REFLEXIE
ISSN: 1336-9202 (online)
2025, Number 3, Page 45-56

CURRENT CHALLENGES FOR UTILIZATION OF COMBAT UNMANNED GROUND VEHICLES

Pavel ZAHRADNÍČEK, Jan HRDINKA, Karel BÖHM

ARTICLE HISTORY

Submitted: *03.11.2025*

Accepted: *27.11.2025*

Published: *31.12.2025*

ABSTRACT

The article deals with the topic of unmanned ground vehicles, esp. their combat versions. Nowadays, the Ukrainian conflict is still in an active phase, and the warfighting of both sides has developed, including new tools and entities on the battlefield. The intention of the article is wide description and summarisation of current state and close future challenges for combat units and their new elements—unmanned ground vehicles. From scientific tools, open-source analysis, extrapolation of results, and expert assessment based on experiences, results of experiments and terrain tests, and factual logic has been chosen. For completing the information, the the MOOSEMUSS acronym was utilized. The inputs are based on practical and scientific results, combining a holistic approach. The point of view represents the community of users—commanders of manoeuvring units, prospectively equipped by unmanned ground vehicles. As a result, is offered synthetised and generalised overview according to principles of war on tactical utilisation of unmanned ground vehicles. The aim of article is not to analyse isolated experience from experimental polygons or battlefield.

KEYWORDS

Maneuver, Mass, Offensive, Objective, Security, Simplicity, Surprise, Unity of Command, Unmanned Ground Vehicle.

INTRODUCTION

The modern battlefield and the character of warfighting are linked with the necessity of utilizing new technologies and procedures (PIERCE 2004; ZAHRADNICEK & BOTIK 2024; Hybrid Warfare Reference Curriculum Volume I, 2024), which are leading to gaining tactical, operational, and strategic advantages and defeating the enemy (HRDINKA, 2024). One of the tools representing this approach is the utilization of unmanned vehicles. These vehicles, in various modifications, play a more or less supportive role in the current conflict. The reason why and how to reverse this situation is covered by this article.

The article is focused on tactical utilization of combat unmanned ground vehicles (UGVs) as a core element of research. The increasing trend of deployment of UGVs is visible from various sources (HRDINKA et al. 2025, p. 122-123; KOMPAN, 2024; HRNČIAR 2025)

Despite this, the role of UGV on the battlefield is still supportive. The logical prediction is when these systems will play a decisive role.

The article is supported by statements and "open sources" dealing with the Ukrainian conflict. Also, previous studies and experiments are incorporated.

Mostly filled-in methods for researching the composition of the article were open-source analysis, extrapolation of results, and expert assessment based on experiences, results of experiments and terrain tests, and factual logic.

For better structuring the article, the acronym MOOSEMUSS has been used. This acronym represents "Nine principles of warfighting" (Marine Corps Institute (U.S.) 1989) and represents Mass, Objective, Offensive, Security, Economy of Force, Maneuver, Unity of Command, Surprise, and Simplicity. The nine principles of war are aids to a leader as they consider how to accomplish a mission. As opposed to being prescriptive steps or actions that must be accomplished, they are guidelines for conducting operations through all the levels of war: strategic, operational, and tactical (United States Marine Corps 2018, 28-32). Sightless adherence to these principles will not guarantee success, but each deviation increases risk. This principles do not change in time, they were valid in past, are valid now and will be valid in future. What is changeable, are devices, tools, methods and tactical variables, specifically Mission, Enemy, Terrain and Weather, Troops and Support Available, Time Available, Civil Considerations. Therefore, the MOOSEMUSS, as a tool, seems to be a good opportunity to describe current problems of utilization of UGVs. Other descriptors were considered (for. ex. DOTMLPFI, SWOT analysis, PICO analysis, FMEA analysis, DMAIC analysis), but they do not follow viewpoint from perspective or military art at tactical level.

1 MASS

The concept of "concentrating the effects of combat power at the decisive place and time to achieve decisive results." Vital to the concept of mass is having the insight to identify the decisive place and time in which to attack the enemy's critical vulnerability. Concentrated fire power is irrelevant if applied to an objective of no significance. We seek mass to overwhelm the enemy in an attempt to deliver the decisive blow. It applies not only to fires but also to supporting elements as well. It is closely related to economy of force, as force available is limited and we must decide when and where it is appropriate to mass or economize our force.

The UGVs enable support for the mass. The lack of manned teams can be supported by UGVs as fire support elements equipped with grenade launchers, machine guns, or cannons. Second, it can be used for supporting operations and enable manned teams to be deployed in decisive operations. The barriers are lack of autonomy, electronic warfare, and speed of actions and reactions (HRDINKA et al. 2025, p. 131-132). According to current conflict experiences, the combat UGV´s are deployed and in stabilised positions, they fill in gaps between combat outpost of infantry. They support the mass.

Also, current armored vehicles (armored personnel carriers and infantry fighting vehicles) are not equipped with platforms for transporting small UGVs inside the vehicle as part of a section or platoon. This approach is philosophically similar to utilizing antitank rocket launchers as an integral part of the BMP crew (weaponsystems.net). UGVs need to be transported and operated as an integral part of a squad or platoon, which causes utilization at the right time in the right place. The typical tasks, according to ČERNÝ & DROZD (2014), for these elements can be, for example, support by fire, attack by fire, participating in breaching operations, operations for containing, etc. From tests and experiences from operational deployment, they are not ready for utilization in dynamic as a unit performing the main effort.

2 OBJECTIVE

The concept of "directing every military operation toward a clearly defined, decisive, and attainable objective." Related to mass and economy of force, we must know where to mass and where to economize, which is defined by a decisive objective. It is also related to unity of command, as each subordinate must be led by the intent of one commander towards the commonly defined objective. Communication is also critical, ensuring that the elements of the military operation are acting in consonance towards the same end. (Marine Corps Institute (U.S.) 1989).

These demands seem problematic from the perspective of controlling the UGV. The vehicles must be precisely operated. The specific objective, fulfilled task in the right place against the right enemy, can be disrupted by electronic warfare. Therefore, operating via cables or optic cables as an alternative can be a solution. Using lethal firepower has to be adjusted by man; the target must be verified. Combat identification as a fully autonomous process is still not correctly developed.

3 OFFENSIVE

The concept that we, as a fighting force, are continuously focused on "seizing, retaining, and exploiting the initiative." Maintaining an offensive mindset does not imply that we seek to avoid defence. Rather it implies the use of the defence as a temporary expedient to prepare to resume the offense. Offense being the decisive form of combat, it is the method by which we exploit the enemy weakness, impose our will, and determine the course of war (Marine Corps Institute (U.S.) 1989).

The combat UGV´s have abilities to support the “offensive approach”. Their ability to support by fire manoeuvring elements enable concentrate the power in specific direction or axis, enable movement of manoeuvring elements and keeps enemy pinned down. The firepower is limited by type of weapon, because only heavy weapon with amount of ammunition can be mounted on appropriate chassis. Also, real trafficability of chassis can limit the offence. The small UGV´s can be well equipped by grenade-launchers (JANES 2025) or rocket- launchers (MILLER 2025), what from viewpoint of stability is acceptable solution. The machineguns and rifles, mounted at platform, do not have satisfying ration between lethal effect and consumption of ammunition, when they are not equipped with stabilisation, based on terrain experiments (HRDINKA 2025, p.129-130).

The course of action, based on current conflict is presented on picture bellow, where the UGVs conduct the support by fire, during the units manoeuvre.

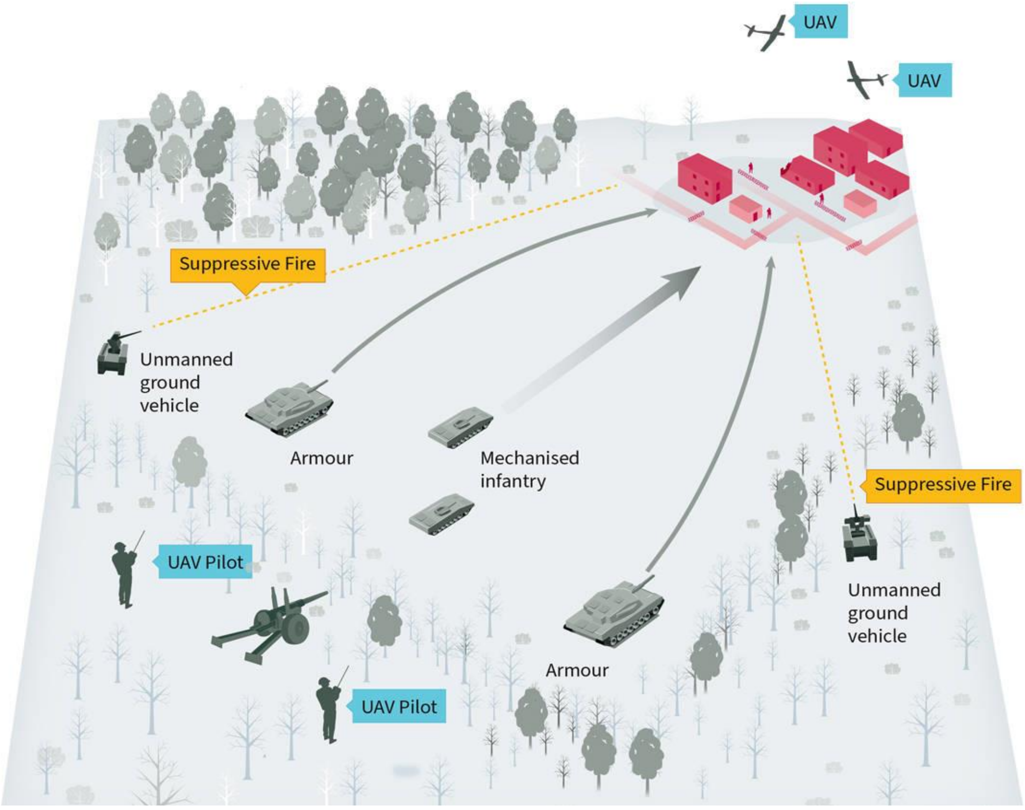


Figure 1 Closing with the Enemy: the role of UGV

Source: Watling, 23 October 2025

4 SECURITY

The concept that we, as a fighting force, are continuously focused on “seizing, retaining, and exploiting the initiative." Maintaining an offensive mindset does not imply that we seek to avoid defense. Rather, it implies the use of the defense as a temporary expedient to prepare to resume the offense. Offense being the decisive form of combat, it is the method by which we exploit the enemy weakness, impose our will, and determine the course of war (Marine Corps Institute (U.S.) 1989).

The combat UGVs have abilities to support the “offensive approach.” Their ability to support by fire maneuvering elements enables concentrating the power in a specific direction or axis, enables movement of maneuvering elements, and keeps the enemy pinned down. The firepower is limited by the type of weapon, because only heavy weapons with an amount of ammunition can be mounted on appropriate chassis. Also, real trafficability of the chassis can limit the offense. The small UGVs can be well equipped with grenade launchers (JANES 2025) or rocket launchers (Miller 2025), which, from the viewpoint of stability, is an acceptable solution. The machine guns and rifles, mounted on the platform, do not have a satisfying ratio between lethal effect and consumption of ammunition when they are not equipped with stabilization, based on terrain experiments (HRDINKA 2025, p.129-130).

5 ECONOMY OF FORCE

The concept of "allocating minimum essential combat power to secondary efforts." This goes hand-in-hand with the concept of mass. In order for us to concentrate decisive combat power at the decisive point, we must know where to economize forces at our secondary efforts. This also implies an acceptance of calculated risk at these secondary efforts. Limited attacks, defense, deceptions, or delaying actions can help us economize forces allowing us to weight the main effort with mass (Marine Corps Institute (U.S.) 1989).

This principle is extremely valid for utilising not only for UAV´s, but also for UGV´s and in fact it is the reason, why to develop unmanned vehicles. Advanced robotic systems, working autonomously or semi-autonomously enable the commanders safe the manpower for deceisive operations or for activities, where is presence of manned teams essential. Good example can be stabilising operations or counter-insurgency operations (HRNČIAR 2018).

6 MANEUVER

The concept of "allocating minimum essential combat power to secondary efforts." This goes hand-in-hand with the concept of mass. In order for us to concentrate decisive combat power at the decisive point, we must know where to economize forces at our secondary efforts. This also implies an acceptance of calculated risk at these secondary efforts. Limited attacks, defense, deceptions, or delaying actions can help us economize forces, allowing us to weight the main effort with mass (Marine Corps Institute (U.S.) 1989).

This principle is extremely valid for utilizing not only UAVs but also UGVs, and in fact it is the reason why to develop unmanned vehicles. Advanced robotic systems, working autonomously or semi-autonomously, enable the commanders to save the manpower for decisive operations or for activities where the presence of manned teams is essential. A good example can be stabilizing operations or counter-insurgency operations (HRNČIAR 2018).

The maneuver is limited. The significant limit is terrain in combination with level of autonomy (KOMPAN 2025). Many scientific studiea are extremely focused on technical solution, but practical impact and results in battlefield are „for discussion“. The remote controlled UGV´s are deployed in current praxis. The idea of combined arms manned-ummanned system is cultivated, and almost every month developed.

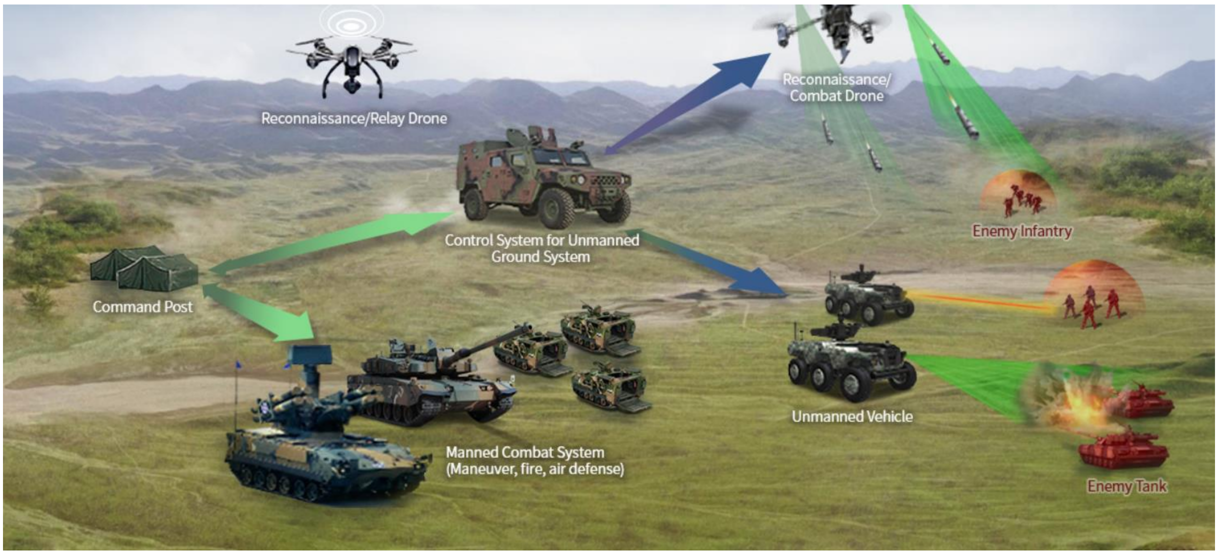

Reconnaissance/Relay Drone
Reconnaissance/ Combat Drone
Control System for Unmanned Ground System
Enemy Infantry
Command Post
Unmanned Vehicle
Manned Combat System (Maneuver, fire, air defense)
Enemy Tank

Figure 2 Combined arms: Dronebot combat system

Source: Dronebot Combat System

The proportions of current battlefield are changed according known doctrines. From this perspective, the aerial and ground unmanned systems are extremly valid, because they support mass, concentration and are able to fill-in gaps and empty corridors. Maneuvring is more probable and the operation dynamics is from perspective of movement is to solve. This prevents the situation, where the forces are generaly „positioning“.

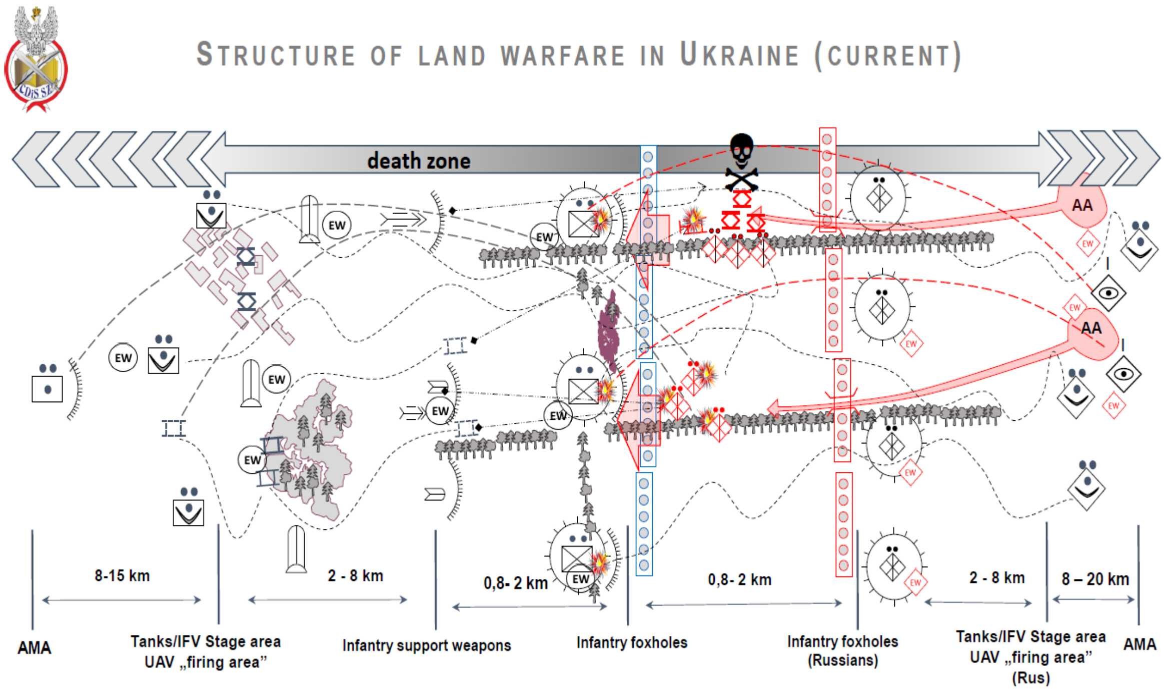


Figure 3 Structure of land warfare Ukraine (current)

Source: Niedźwiecki, 2025

As above mentioned author Niedźwiecki explains,the battlefield leads the commanders to solve, how to boost the movement, dynamics and unblock current general state. Based on discussions, the authors can uderline results from discussion of Future Land Forces conference and recommned: deploy ammount of small hi-tech object on battlefield, duouble or shift some capabilities on drones, fires (combination of massive and precise) will be essential, counter drone capabilities unblock the positioning, electronic warfare needs to be the ability of small unit, not the ability of achelons and formations.

7 UNITY OF COMMAND

Best exemplified by commander’s intent, “Unity of Command” is the concept that “for every objective, we ensure unity of effort under one responsible commander.” Mass, economy of force, and maneuver would be impossible without the vision of a single leader. To ensure that vision is carried to the lowest levels while still allowing for flexibility and initiative, we use commander’s intent. It allows for and leverages mass, objective, and economy of force at the decisive point.

The autonomy of vehicles and “un-crewing” makes pressure to keep them under control, using the principal of unity of command. The task must be clearly understood, and the vehicle's behavior has to follow the orders. In case of adding the vehicles as a part of platoons, every battalion will be reinforced by minimally 9 new UGVs, which can represent the firepower of a large platoon or small company, based on weapon systems. Exponential increasing of UGVs will require a robust command and control system and upgrading related functions, such as intelligence, surveillance, target acquisition, and reconnaissance. Situational awareness and operational picture will be more dense, and also inputs and analyzing incoming messages will be the next task for small unit leaders. The capacity of communication systems can be a challenge, similarly like in the Ukrainian conflict (SpaceX Starlink internet isn't fast enough for Ukraine's combat robots, 2025).

8 SURPRISE

The concept that we seek to “strike the enemy at a time or place or in a manner for which he is unprepared.” It does not require the enemy to be caught unaware, but rather that he becomes aware too late to react effectively. May include the use of speed (maneuver in time), unexpected forces (mass), operating at night (psychological and technological maneuver), deception (psychological maneuver), security, variation in techniques, and use of unfavorable terrain (spatial maneuver) (Marine Corps Institute (U.S.) 1989).

The definition of surprise can be filled by the implementation of UGVs into structures of combat units as well. The “unknown” elements on the battlefield have not only lethal power but also psychological. Based on experimentation by the Department of Tactics, University of Defence, the manned units are attracted by the movement of UGVs. Similarly, like by the presence of drones. This can take away the vigilance of forces and create conditions for tactical surprise. Additionally, the movement to contact, in order to find the enemy or disrupt the enemy, is a logical opportunity for how to implement this characteristic.

9 SIMPLICITY

The concept that the preparation of “clear, uncomplicated plans and clear, concise orders ensures thorough understanding” and therefore ease of execution. Plans and orders should be as simple and direct as the situation and mission dictate. This reduces the chance of misunderstandings that inject internal friction and therefore cause ineffective execution. Ceteris paribus (all variables being equal), the simplest plan is preferred (Marine Corps Institute (U.S.) 1989).

The simplicity of utilization is crucial when using a number of sophisticated systems. Adequate mission tasks, limiting possible failures, are necessary to order. Commanders have to reduce the risks of failures. Again, adequate tasks, right timing, and having contingency plans are the way to reduce possible mistakes. The operators, controlling UGVs from a distance, do not have a 3D view, like the foot soldier. The UGVs are not so quick in reaction or are extremely quick in reactions. It can cause unpredictable situations.

CONCLUSION

The UGVs, similarly to other elements on the battlefield, have to adopt principles of warfighting because they are part of a warfighting organism—a hybrid military system.

Overall output from this study is that UGVs are not developed for autonomous acting from the viewpoint of tactics. They can be able to conduct „isolated" actions, but they are not fully technically prepared to replace soldiers or crews. On the other hand, they demonstrate opportunity, how to support their own capabilities, and how to increase combat effectiveness. The core of development is in experimentation in real or almost real situations and adapting not only machines but also operators and commanders (ZAHRADNÍČEK et al. 2023).

The authors are convinced that the principles described in the acronym MOOSEMUSS are influencing each other according to the matrix. Therefore, the real abilities of UGVs are related also.

Table 1: MOOSEMUSS matrix

	M	**O**	**O**	**S**	**E**	**M**	**U**	**S**	**S**
M	x								
O		x							
O			x						
S				x					
E					x				
M						x			
U							x		
S								x	
S									x

Source: Own

The key message of the article was described in chapter 6. Not only unmanned systems, but whole approach to modern warfare has to be adopted. The combined arms, equipped by family of drones, operated in planned frequence, sequence, tempo in small groups or separately will be essitial. The battlefield will be inflated, according to new abilities of devices (esp. range of fire, precision). This creates significant change comparing valid doctrines from WW2 to 2022.

REFERENCES

CLAUSEWITZ, C. von, 2008. *O válce* Vyd. 3., V nakl. Academia 1., Praha: Academia.

DANIEL M. Carroll, MIKELL, K. & DENEWILER, T., 2004. <title>Unmanned ground vehicles for integrated force protection. In *Proceedings of SPIE, the International Society for Optical Engineering/Proceedings of SPIE*. pp. 367-377. https://doi.org/10.1117/12.553045

Dronebot Combat System. *Hanwha Systems* [online]. [cit. 2025-11-28]. Dostupné z: https://www.hanwhasystems.com/en/business/defense/land/dronebot_index.do

DROZD, J. et al., 2021. Effectiveness evaluation of aerial reconnaissance in battalion force protection operation using the constructive simulation. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 20(2), pp.181-196. https://doi.org/10.1177/15485129211040373

Grenade launcher RWS integrated onto THeMIS UGV for Ukraine. *Janes*. Available at: https://www.janes.com/osint-insights/defence-news/defence/grenade-launcher-rws-integrated-onto-themis-ugv-for-ukraine [Accessed October 29, 2025].

HRDINKA, Jan. 2024. "Bezpilotní pozemní prostředky ve válkách a konfliktech: revize a současný vývoj." In 18. doktorandská konference: Nové přístupy k zajištění bezpečnosti státu, 74-85. Brno: Univerzita obrany. https://lib.unob.cz/KONFERENCE/DK/DK_Sbor

HRDINKA, J. et al., 2025. Possibility of Supporting the Activity of Infantry Units with Combat Unmanned Ground Systems During an Attack Operation. *Vojenské rozhledy*, 34(1), pp.120-135. https://doi.org/10.3849/2336-2995.34.2025.01.120-135

HRNČIAR, M., 2018. The Counter Insurgency Operating Environment. *International conference KNOWLEDGE-BASED ORGANIZATION*, 24(1), pp.87-92. Available at: https://www.sciendo.com/article/10.1515/kbo-2018-0013 [Accessed July 21, 2023]. https://doi.org/10.1515/kbo-2018-0013

HRNČIAR, Michal, Jaroslav KOMPAN a Jan NOHEL, 2025. The future of the battlefield: Technology-driven predictions in the land domain. *Revista Científica General José María Córdova* [online]. Escuela Militar de Cadetes Jose Maria Cordova, 2025-3-6, **23**(49), 277-296 [cit. 2025-11-28]. ISSN 2500-7645. Dostupné z: doi:10.21830/19006586.1323

Hybrid Warfare Reference Curriculum Volume I [online], 2024. Ludovika Egyetemi Kiadó, 2024-5-13 [cit. 2025-11-28]. ISBN 9789636530327. Dostupné z: doi:10.36250/01195_00

KOMPAN, Jaroslav, Michal HRNČIAR a Daniel BREZINA, 2025. Technological Aspects of Military Mobility Support. In: *Lecture Notes in Intelligent Transportation and Infrastructure* [online]. Cham: Springer Nature Switzerland, s. 157-166 [cit. 2025-11-28]. ISBN 9783031853890. ISSN 2523-3440. Dostupné z: doi:10.1007/978-3-031-85390-6_16

KOMPAN, Jaroslav, Milan TURAJ a Michal VAJDA, 2024. Operational Environment. In: *Hybrid Warfare Reference Curriculum Volume I* [online]. Ludovika Egyetemi Kiadó, 2024-5-13, s. 99-128 [cit. 2025-11-28]. ISBN 9789636530327. Dostupné z: doi:10.36250/01195_06

Marine Corps Institute (U.S.), 1989. Tactical Fundamentals.

MILLER, S., PLA integrates armed FPV unmanned vehicles in exercise. *Asianmilitaryreview.com*. Available at: https://www.asianmilitaryreview.com/2025/08/pla-integrates-armed-fpv-unmanned-vehicles-in-exercise-foc/ [Accessed October 29, 2025].

NIEDŹWIECKI, Artur, 2025. *DYNAMICS OF CHANGE FUTURE WARFIGHTING IN THE CONTEXT OF LESSONS LEARNED FROM UKRAINE WAR: Conferrence Future Land Forces 2025*. DOCTRINE AND TRAINING CENTRE OF THE POLISH ARMED FORCES.

NOHEL, J. et al., 2023. Area reconnaissance modeling of modular reconnaissance robotic systems. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 22(4), pp.503-519. https://doi.org/10.1177/15485129231210302

NOHEL, J., STODOLA, P. & FLASAR, Z., 2021. Combat UGV Support of Company Task Force Operations. In *Lecture Notes in Computer Science*. Cham: Springer International Publishing, pp. 29-42.

NOHEL, Jan & ZAHRADNÍČEK, Pavel & KOMPAN, Jaroslav & RAK, Luděk & HRADSKY, Ludovit. (2025). Automated processing of up-to-date tactical geographical information as a key to UGS autonomy. 1-8. https://doi.org/10.1109/KIT67756.2025.11205438

NOHEL, J. et al., 2021. Possibilities of Modelling the Coordinated Maneuver of Units in Difficult Terrain Conditions. In *2021 Communication and Information Technologies (KIT)*. IEEE, pp. 1-5. https://doi.org/10.1109/KIT52904.2021.9583742

PIERCE, T., 2004. *Warfighting and Disruptive Technologies: Disguising Innovation*, Routledge.

PULTAROVA, Tereza, 2025. *SpaceX Starlink internet isn't fast enough for Ukraine's combat robots*. Online. In: Space.com. Dostupné z: https://www.space.com/space-exploration/satellites/spacex-starlink-internet-isnt-fast-enough-for-ukraines-combat-robots?sznclid=-pOex8vIyczKysLNw8jMwsjCzcPOys-GjsfLzc7Kz87NyMvC1MnLwoaOn8fLzczLzcvPy8nO1MjLyoaZx8zJzMjKyM3CvsO-zM2-v8vKysPDyry5wrvMws64yMi8&u. [cit. 2025-10-29].

United States. Marine Corps, 2018. *Warfighting*, Marine Corps Association.

WATLING, Jack, 23 October 2025. Emergent Approaches to Combined Arms Manoeuvre in Ukraine. In: *RUSI* [online]. [cit. 2025-11-28]. Dostupné z: https://www.rusi.org/explore-our-research/publications/insights-papers/emergent-approaches-combined-arms-manoeuvre-ukraine

ZAHRADNÍČEK, P.& BOTÍK,M. 2024. Technologies in the Ukrainian Conflict: Reflection and Perspectives from Viewpoint of Combat Unit's Utilization. *Challenges to National Defence in Contemporary Geopolitical Situation*, 1(1). https://doi.org/10.3849/cndcgs.2024.351

ZAHRADNÍČEK, P., RAK, L. & ZEZULA, J., 2022. Budoucí prostředí a robotické autonomní systémy. *Vojenské reflexie*, 17(2), pp.56-72. https://doi.org/10.52651/vr.a.2022.2.56-72

ZAHRADNÍČEK, P. et al., 2023. Modern Battlefield and Necessary Reflection in Military Leader's Education and Training. Vojenské rozhledy, 32(4), pp.110-122. https://doi.org/10.3849/2336-2995.32.2023.04.110-122

ZŮNA, P. 2021. *Paradigmata vojenské taktiky*, Litomyšl: H.R.G. spol. s r.o.

COL Pavel ZAHRADNICEK
University of Defence
Kounicova 65, Brno
Telephone: +420 724 255 307
E-mail: pavel.zahradnicek@unob.cz

Jan HRDINKA,
University of Defence
Kounicova 65, Brno
E-mail: jan.hrdinka@unob.cz

Karel BÖHM
University of Defence
Kounicova 65, Brno
E-mail: karel.bohm@unob.cz

DOI: https://doi.org/10.52651/vr.a.2025.3.57-69

VOJENSKÉ REFLEXIE
ISSN: 1336-9202 (online)
2025, Number 3, Page 57-69

EMERGING AND DISRUPTIVE TECHNOLOGIES AND DISINFORMATION IN UN PEACEKEEPING MISSIONS

Elisabeta-Emilia HALMAGHI, Alin CÎRDEI, Ileana-Gentilia METEA, Daniela CĂRUȚAȘU

ARTICLE HISTORY

Submitted: *05.11.2025*
Accepted: *27.11.2025*
Published: *31.12.2025*

ABSTRACT

Emerging and disruptive technologies are increasingly present in our lives, determining the increase in people's living standards and the progress of society. The influence of this type of technologies is present in both the civilian and military environments. In the military environment, by transforming into capabilities, the impact will be significant on defense institutions, but also on classic security strategies, military doctrines, operational concepts, wars. In this paper, using the bibliographical and analytical method, it will be highlighted how emerging and disruptive technologies can be used by hostile forces to increase disinformation and uncertainty in conflict areas where peacekeeping missions are carried out under the auspices of the UN. Personnel participating in UN missions must identify the signs of a disinformation campaign as early as possible and have the necessary knowledge to combat it.

KEYWORDS

disinformation; disruptive technologies; emerging technologies; false information; peacekeeping missions; UN.

INTRODUCTION

In an era where information circulates extremely quickly thanks to the online environment, a new major challenge has emerged: disinformation. This challenge manifests itself at all levels, in all areas, and contributes to the manipulation of people. Disinformation spreads rapidly online, but also offline and in the media.

Emerging and disruptive technologies are changing the way the world works. In their use, emerging and disruptive technologies present both advantages and disadvantages and "will have a major impact, with specific effects and risks related to the new products and services that could emerge and disrupt markets, as well as how businesses will be adapted, transformed and run in accordance with the new business model" (Coman et al., 2024).

The paper aims to present the role that emerging and disruptive technologies play in the propagation of disinformation in UN peacekeeping missions.

To achieve the objective, we presented and analyzed, based on the study of the bibliography and our own observations, the importance of emerging and disruptive technologies in military activities and their role in the propagation of disinformation during the conduct of UN peacekeeping missions.

1 EMERGING AND DISRUPTIVE TECHNOLOGIES – TECHNOLOGIES THAT INCREASE THE RESILIENCE OF PEACEKEEPING OPERATIONS

Among the first researchers to note the disruptive nature of technological change was Joseph Schumpeter. He noted in 1939 that this disruptive nature of technological change could lead to waves of "creative destruction" (Chandra Shekar, Anjali, Pavithra, 2017). Many of the technologies that define the modern era (computers, nuclear power, space-based ICT systems and GPS, etc.) emerged as a direct result of public investment driven by geopolitical competition and the dynamics of the arms race between the US and its allies, and the Soviet Union, during the Cold War. The most striking difference in the nature of research and development in science and technology was represented by the increased volume of private investment in so-called "dual-use technologies", usually reserved for civilian purposes but with notable military applications (Vincić, 2021).

Currently, emerging and disruptive technologies (EDT) are increasingly part of our lives, changing the way the world works and "driving societal progress and increasing the standard of living of the individual" (Popescu, 2021, p. 221). These technologies, which come with both opportunities and challenges, are expected to reach maturity in the next 20 years (Popescu, 2021, p. 2019). and have an increasing impact on security and the armed forces. They allow the armed forces to "become more effective, resilient, cost-efficient and sustainable as well as address immediate capability shortfalls and deliver on their capability targets" (NATO, 2025) changing the nature of war (Mills, 2023, p. 4). Beyond the positive impact, EDT present "a huge threat to society, both civil and military, from their misuse" (The Geostrata, 2024).

Emerging technologies are considered to be those technologies that require longer time horizons (between 10 and 20 years) to mature and whose development trajectories are currently less certain (Vincić, 2021).

Disruptive military technology represents "an improved or completely new technology capable of producing fundamental changes to traditional models of security and defense" (Iancu, 2019) and is in a more advanced state of technological maturity already having/expected to have significant and potentially revolutionary impacts on the nature of warfare and collective defense and security in the period 2020-2040 (Vincić, 2021).

These technologies, by transforming into military capabilities, will have an impact on classic security strategies, military doctrines, operational concepts, wars, but also on the organization of defense institutions.

Like any product, disruptive technologies have four life phases (Figure 1).

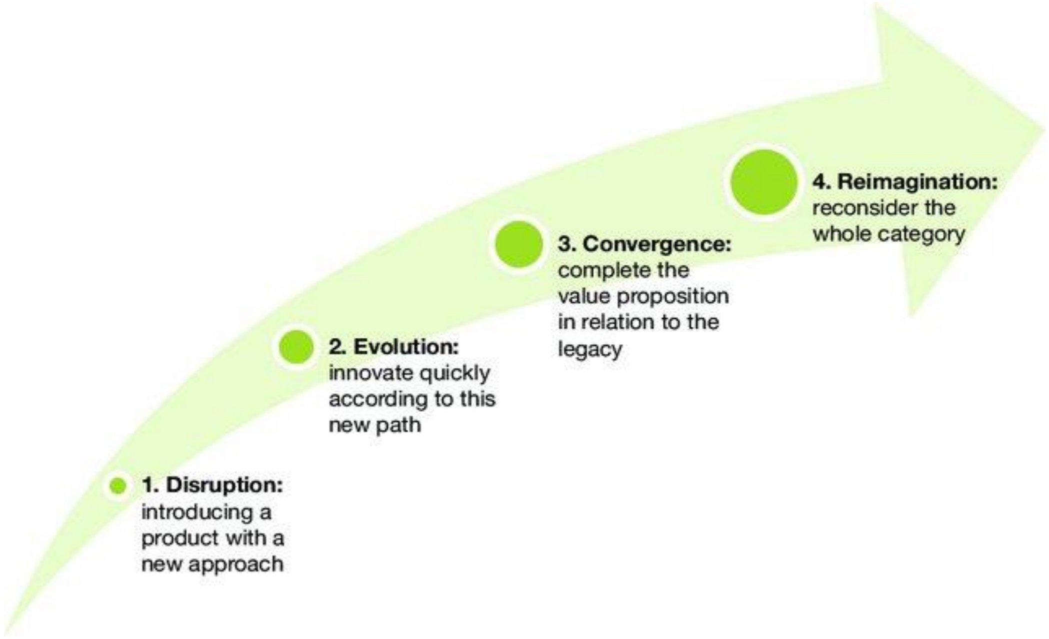

1. Disruption: introducing a product with a new approach
2. Evolution: innovate quickly according to this new path
3. Convergence: complete the value proposition in relation to the legacy
4. Reimagination: reconsider the whole category

Figure 1 Phases of disruptive technologies
Source: Veuger, 2018

The phases of disruptive technologies are presented in Tab. 1, where column 2 lists the characteristics of the disruptor evolving from a niche solution to an asset used in both civilian and military environments, and column 3 lists the prototype result.

Table 1 Phases of disruptive technologies

Phase	Disruptor	Incumbent / Prototype
Disruption of the established order	Introduce a new product with a well-defined approach, recognizing that it may not meet all the needs of the entire existing market, but it improves on state-of-the-art technology.	The new product/service is not relevant to existing customers or the market (also known as "denial")
Rapid linear evolution	Adds features and capabilities, increasing value based on feedback from a group of early adopters.	Compares the complete product with its own new product and identifies defects (also known as "validating")
Convergence. Completely reinvented product	Sees an opportunity to broaden the customer base by attracting new companies. Recognizes the limitations of its	Disruptive core features are added to the existing product line to demonstrate attention to future trends while minimizing disruption

Phase	Disruptor	Incumbent / Prototype
	new product and learns from previous practices, but applies them in a new way. Potential risks are continuously addressed with new technologies and business models, and the focus shifts to the "installed base" of the already existing order.	to existing customers (also known as "competition"). A potential risk is that disruptive products are not recognized as truly valuable or do not offer opportunities relative to the limitations of existing products.
Completely reinvented product	Approaching a decision point because new entrants to the market can benefit from everything the new product has demonstrated, without considering existing customers. Focusing more on market legacy or continuing the path already taken.	It is too late to react. Begins defining the new product as part of a new market and the existing product as part of a larger, existing market (also known as "retraction").

Source: Processing after Veuger, 2018

Emerging and disruptive military technologies are: artificial intelligence (AI), hypersonic systems, autonomous systems, biotechnologies and human enhancement technologies, quantum technologies, space, next-generation communication networks, energy and propulsion, new materials and their production (NATO, 2025).

Artificial intelligence is a catalyst for the development of emerging and disruptive technologies and a basic element in the implementation of other technologies in the military field, because systems equipped with artificial intelligence will be able to perform analyses, identify threats, solutions and courses of action, assist decision-making or even make decisions independently, thus optimizing other systems and acting as an amplifier of human strength and intelligence (Cîrdei, 2025).

Technologies are developing at a dizzying pace, and their impact on all areas is unimaginable. Artificial intelligence is an engine of development of all other areas and is driving the development of new emerging and disruptive technologies. Moreover, artificial intelligence will allow for the achievement of quantum supremacy, thus creating the conditions for tasks and activities that normally take a long time to be completed in a few seconds. The fundamental question that arises here is if and when this technology will become widely accessible, because then every terrorist, insurgent or other entity or organization will have access to almost unlimited computing power.

When quantum power is widely available, its impact on military operations will be immense. Taking advantage of this emerging technology, the speed, scale, and quality of disinformation campaigns will be so great that it will be almost impossible to identify and very difficult to combat, because it will be a significant challenge to distinguish between real and simulated actions, between those specific to current activities and legitimate military operations and those that support disinformation actions.

These technologies are fundamentally changing the missions of the United Nations (UN) to maintain peace. In general, UN peacekeeping missions aim to assist states in the transition from conflict to peace. In carrying out peacekeeping missions, the UN has "unique strengths, including legitimacy, burden-sharing, and the ability to deploy troops and police from around the world, integrating them with civilian peacekeeping forces to fulfill a range of mandates set by the UN Security Council and the General Assembly" (United Nations Peacekeeping, 2025c).

If the Action for Peacekeeping Initiative aimed to strengthen, secure and make UN missions more effective, A4P+ aims to accelerate its implementation (Figure 2). To this end, "concrete measures have been adopted across all areas of A4P+, from improving the safety, security and well-being of our personnel to increasing the participation and expanding the role of women in our missions" (United Nations Peacekeeping, 2025a).

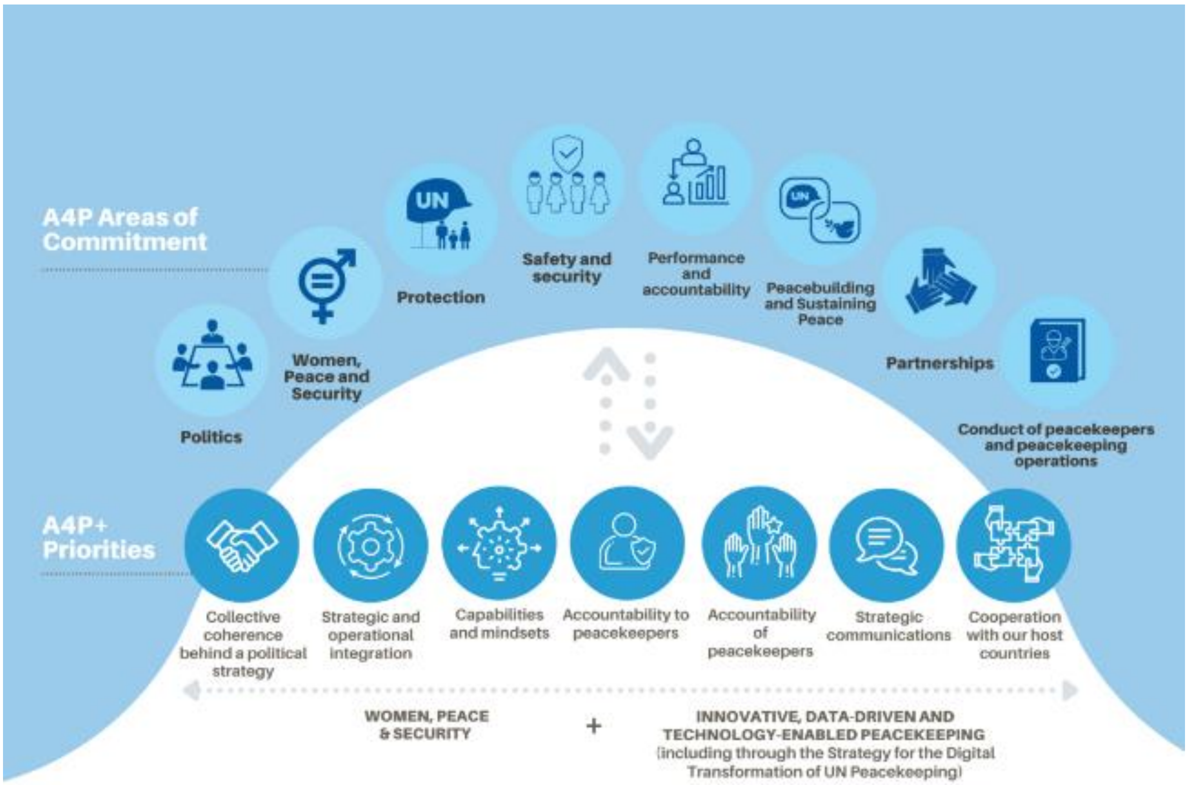

A4P Areas of Commitment
Politics
Women, Peace and Security
Protection
Safety and security
Performance and accountability
Peacebuilding and Sustaining Peace
Partnerships
Conduct of peacekeepers and peacekeeping operations
A4P+ Priorities
Collective coherence behind a political strategy
Strategic and operational integration
Capabilities and mindsets
Accountability to peacekeepers
Accountability of peacekeepers
Strategic communications
Cooperation with our host countries
WOMEN, PEACE & SECURITY
+
INNOVATIVE, DATA-DRIVEN AND TECHNOLOGY-ENABLED PEACEKEEPING (including through the Strategy for the Digital Transformation of UN Peacekeeping)

Figure 2 Action for Peacekeeping and Action for Peacekeeping+

Source: United Nations Peacekeeping, 2025c

It should also be borne in mind that threats to peacekeeping personnel do not only come from the physical environment and do not only endanger the physical safety of the personnel. In the age of technology and the Internet, military and civilian personnel participating in peacekeeping operations are faced with risks arising from the cyber environment that can have faster and more intense effects than actions carried out in the physical environment, even using military means.

Cyber threats and those specific to information warfare are, most of the time, invisible and therefore difficult to counter, especially due to the fact that the target would be aware that it is subject to an attack only after the attack is underway or even after it has been completed. Thus, the attention of decision-makers and peacekeeping personnel will not be focused on preventing attacks, but on countering them and limiting their effects and damage.

That is why personnel participating in peacekeeping missions must have training in cyber and information operations in order to be aware of the danger they represent, the damage they can cause and the indications of such hostile actions in order to be able to counter them. While cyber threats and information operations are not new in the military field, we can observe that new confrontations are taking on a hybrid character, because the environments of confrontation, the methods of conducting military actions and their targets are increasingly diverse, and their countering is increasingly difficult.

Hybrid threats are becoming a constant of current activities and especially of the actions of the armed forces that must get used to operating in such conditions, marked by uncertainty, volatility, unpredictability and multidimensional and multidomain risk. Hybrid threats are a significant concern today due to their ability to exploit vulnerabilities in interconnected, open societies, using a combination of conventional and unconventional tactics. These threats are increasingly visible in all domains and are predominantly manifested in parallel with classical military or peacekeeping actions, with the aim of creating insecurity, distrust and suspicion.

Technology and connectivity have significantly amplified the scope and impact of hybrid threats on armed forces and their ability to conduct military actions. The ability to disseminate disinformation on a large scale, to conduct sophisticated cyber-attacks, to exploit global interdependencies and to coordinate operations in real time are key factors that make hybrid threats particularly challenging in the modern era.

The UN is currently involved in 11 peacekeeping operations led by the Department of Peacekeeping Operations. These are mainly conducted on the African continent in Western Sahara, Congo, Central African Republic, Abyei, and South Sudan. Other areas where peacekeeping operations are conducted include: Kosovo, Cyprus, Lebanon, Golan, Middle East, on the border between India and Pakistan. As of 31 July 2025, 68,255 personnel were involved in the 11 peacekeeping operations (United Nations Peacekeeping, 2025b).

The nature of contemporary conflicts has evolved, requiring continuous adaptation of peacekeeping operations. Despite the fact that this adaptation is in continuous dynamics, UN peacekeeping missions are affected by disinformation.

UN-led missions, regardless of the geographical area in which they are deployed, are exposed to hybrid threats and disinformation actions that are directly directed against the mission and participating personnel, but which also indirectly affect the efficiency and legitimacy of UN forces by targeting the local population, political decision-makers and international public opinion, through coordinated and well-planned actions, which aim to achieve short- and medium-term effects. The initiators of disinformation actions use the advantages offered by modern technologies, especially artificial intelligence, to prepare and carry out real disinformation campaigns, with minimal effort and maximum potential benefits.

2 DISINFORMATION IN UN PEACEKEEPING MISSIONS

Disinformation is not a new phenomenon, but given the dynamics in the communications area and the continuous development of digital platforms, the large-scale use of AI (voice and facial recognition systems, image analysis software, virtual assistants, etc.), the scale of the problem is amplified, which makes it even more difficult to trust information and to present real facts in conflict situations.

What is new is that digital technology has allowed the creation, dissemination and amplification of false or manipulated information by various actors, for ideological, political and/or commercial reasons, at a scale, speed and coverage never seen before. Interacting with real-world political, social and economic grievances, disinformation can have serious consequences for democracy because it distorts public debate, polarises society and prevents people from making informed choices, free from interference and manipulation (European Parliament, 2025), incites hatred, discrimination and violence, prevents people from meaningfully exercising their rights and destroys their trust in governments and institutions (United Nations 2021).

Disinformation (false information that is deliberately created to cause harm to an individual, social group, organization, or country), misinformation (false information that appears in the public domain without the intention of causing harm by the people spreading it), and malinformation (fact-based information used to cause harm to an individual, social group, organization, or country) (United Nations 2023) have become a serious threat, both to members of society and to institutions. The boundary between the three is volatile (Figure 3), and what began as disinformation tends to turn into misinformation as it spreads, since most people do not share false information with malicious intent.

There is an important difference between fake news and disinformation (Tătaru et al., 2024), as false information can blur into disinformation when seemingly true information is lacking nuance or context (Trithart, 2022).

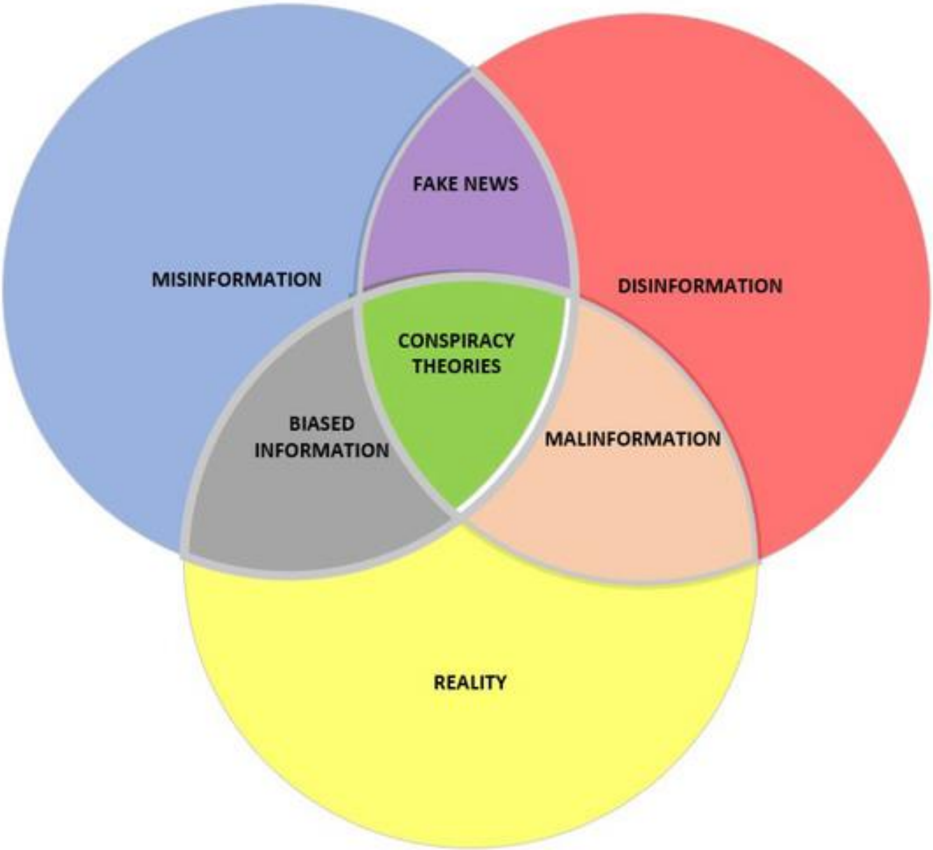


Figure 3 The Disinformation – Misinformation - Malinformation Connection
Source: Tătaru et al., 2024

In the case of UN peacekeeping operations, the increase in disinformation can undermine trust in peacekeeping missions, exacerbate conflicts and encourage violence against UN personnel, limit the mobility and expansion of peacekeeping missions, compromising the protection of civilians. The number of disinformation has increased in recent years and includes (also false) accusations that UN peacekeepers support terrorist groups, traffic in arms and/or human beings, or exploit natural resources. Disinformation about the work of UN peacekeepers is not new, but in recent years, thanks to social media, it has spread at an accelerated pace. Based on public frustration, but also on real cases of mistakes or misconduct by UN peacekeepers, anti-UN disinformation makes it difficult to implement the mandates of peacekeeping operations and endangers the safety of peacekeepers (Trithart, 2022).

For example, in early 2025, M23, with the support of Rwandan armed forces, launched large-scale offensive operations in eastern Democratic Republic of Congo. During the offensive, women peacekeepers were threatened with rape and other acts of sexual violence, following an online disinformation campaign, which affected their safety and freedom of movement. This made it difficult to restore security to Congolese communities.

Disinformation is a consequence of the use of advanced technologies aimed at resisting, hindering, slowing down and annihilating UN missions considered beneficial in their areas of operation, but which contradict opposing interests. Mobile phones used as explosive devices, unmanned combat aircraft or cyber-attacks are realistic attack scenarios that are becoming increasingly relevant with digitalization. The figures and challenges show that the UN must not only promote peace and security, but also protect its personnel from threats (Parlamentul European, 2022).

However, there are also logistical issues, as access to modern technology is limited in some conflict zones. Furthermore, overuse of technologies can lead to dependency, which can jeopardize mission success if systems fail.

UN personnel engaged in peacekeeping missions can mitigate the effects of disinformation in the following ways (Stockholm International Peace Research Institute, 2023):

a) Understand and address the roles of different actors when it comes to the spread of mis- and disinformation. There are situations where government officials or civil society representatives challenge the legitimacy and implementation of the mandate of UN operations. In this case, it is necessary for the UN Security Council to provide more guidance and political support to the peacekeeping mission.

b) Recognize that multiple narratives may exist within a country and analyse who owns them. Understanding local culture and history, the causes of conflicts, provides a holistic perspective on the conflict. To better understand the context, it must be borne in mind that in any society there are multiple voices that influence a country politically, economically and socially: the host government, local communities, diaspora. Therefore, it is necessary for UN members to be aware of the sources of information and their potential biases.

c) Analysis of the root causes of a shifting media landscape. Modern conflicts are characterized by a dynamic media environment. Therefore, for propaganda purposes and the dissemination of contradictory information, governments, local communities, and the diaspora fund media institutions.

d) Keep investing in mission-wide communication strategies. Providing information in the media about the mission's role and purpose can help counter fake news and disinformation campaigns. Strategic communication is also essential, and therefore training senior mission leaders in communication and media is an asset.

e) Whole of mission approach. A proactive approach is needed, where the risk of disinformation is considered for the "whole mission". Therefore, for the safety of personnel and to support the implementation of the peacekeeping operation, disinformation should be part of the planning and decision-making process.

f) UN peace operations are complex and large, involving actors with different social, language and cultural settings. The cultural, social and linguistic gap between peacekeeping personnel and members of local communities leads to increased distrust among the indigenous population, undermines the legitimacy of the mission and increases disinformation. By improving linguistic, cultural and social understanding, better conditions for dialogue arise, which leads to transparency, reduces disinformation and increases the trust of local community members in the role of the peacekeeping mission.

g) Keep in mind that criticism of the UN is not always mis- or disinformation. Engaging in dialogue with local community members is essential for the successful implementation of peacekeeping missions. This requires that the information transmitted by UN personnel is accurate, impartial and accessible to communities. That is why it is important to support the rule of law in host countries, train journalists, support independent media and civil society organizations.

Disinformation and propaganda actions take place over time and target both the forces participating in peacekeeping operations, the population and decision-makers. The first step is to create a favorable climate for these actions to be carried out successfully. After the framework is created and a core of supporters and sympathizers is formed, from among the population or even influential people from different fields and political decision-makers, the actual action begins, exploiting the weaknesses of the system and attacking the essential points of the peacekeeping forces.

Once the action is launched, by using means of influence, propaganda and disinformation, misleading, etc., the attackers focus their efforts on achieving the objectives and achieving the desired end state, affecting the ability of the peacekeeping forces to fulfill their mission and affecting the image and respect they enjoy locally and among the international community.

CONCLUSION

The weaponization of digital communications and social media poses new challenges in identifying and countering hostile influences that negatively impact UN peacekeeping operations. Today's peacekeepers not only face disinformation in their operational contexts, but are increasingly becoming targets of disinformation campaigns. Such campaigns are often designed to erode trust in peacekeeping operations, delegitimize international interventions, and deepen divisions in conflict regions.

By jeopardizing the safety and security of UN peacekeepers, disinformation, along with hate speech, limits the mobility and reach of peacekeeping operations, thereby reducing the operations' ability to protect civilians in the host country.

In the case of conflicts in fragile democracies through disinformation, social media can decisively influence how, when and if a conflict manifests. The spread of false information online and in the media with the intention of misleading the public poses increased risks to the well-being of people and society in general. Disinformation polarizes society, jeopardizes the implementation of economic and social policies, and undermines trust in state institutions and democracy.

To combat disinformation, it is necessary for people to develop critical thinking skills and be digitally literate. Through the two components, they will be able to identify and combat the spread of false and/or misleading information. However, the use of social media and AI as a weapon remains a challenge for future work in the field of peace and security.

REFERENCES

CÎRDEI, A. 2025. Folosirea inteligenței artificiale în operațiile militare. In: CÎRDEI, A., BOJOR, L. *Impactul tehnologiilor emergente asupra securității naționale*, Editura Academiei Forțelor Terestre „Nicolae Bălcescu", Sibiu, 2025.

COMAN, M.-M. - KIFOR, C.V. - PIELE, C. 2024. Exploring the Impact of Emerging and Disruptive Technologies Development on Evolution of Industry 5.0. In: *International conference KNOWLEDGE-BASED ORGANIZATION. Nicolae Balcescu Land Forces Academy*, 2024, Vol. 30, No. 3. 49-57. Available at: https://doi.org/10.2478/kbo-2024-0084

European Parliament. 2025. Disinformation: 10 steps to protect yourself and others, Published: 05-06-2025. Available at: https://www.europarl.europa.eu/topics/en/article/20250603STO28720/disinformation-10-steps-to-protect-yourself-and-others

CHANDRA SHEKAR, N. - ANJALI, K. - PAVITHRA, A. 2017. Disruptive Technologies. In: *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)*, 2017, Vol. 4, No. 3. 81-83. ISSN (Online) 2394-2320. Available at: https://www.technoarete.org/common_abstract/pdf/IJERCSE/v4/i3/Ext_23047.pdf

IANCU, N. 2019. Noul dicţionar al apărării: tehnologiile disruptive, 29 iulie 2019. In: Monitorul Apărării și al Securității. Available at: https://monitorulapararii.ro/noul-dictionar-al-apararii-tehnologiile-disruptive-1-21024

MILLS, C. 2023. Emerging and disruptive defence technologies. Commons Library Research Briefing, 13 November, 2023, House of Commons Library. Available at: https://commonslibrary.parliament.uk/research-briefings/cbp-9184/

NATO, 2025. Emerging and disruptive technologies. Last updated: 25 Jun. 2025. Available at: https://www.nato.int/cps/en/natohq/topics_184303.htm

Parlamentul European. 2022. Securitate cibernetică, principalele amenințări. 2022. Available at: https://www.europarl.europa.eu/topics/ro/article/20220120STO21428/securitate-cibernetica-principalele-amenintari

POPESCU, S. 2021. Impactul tehnologiilor emergente și disruptive asupra domeniului militar. In: Conferința Științifică Internațională Gândirea Militară Românească, Ediția a III-a, 2021. Available at: https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2021%20gmr/2021/4%20proceedings%202021/POPESCU.pdf. https://doi.org/10.55535/GMR.2021.4.12

Stockholm International Peace Research Institute. 2023. Tackling mis- and disinformation: Seven insights for UN peace operations. 2023. Available at: https://www.sipri.org/commentary/blog/2023/tackling-mis-and-disinformation-seven-insights-un-peace-operations

TĂTARU, G.-C. - DOMENTEANU, A. - DELCEA, C. - FLORESCU, M. S. - ORZAN, M. - COTFAS, L.-A. 2024. Navigating the Disinformation Maze: A Bibliometric Analysis of Scholarly Efforts. In: *Information*, 2024, Vol. *15*, No. 12. 742. Available at: https://doi.org/10.3390/info15120742

The Geostrata, 2024. Emerging and Disruptive Technologies in Defence, Feb 27, 2024. Available at: https://www.thegeostrata.com/post/emerging-and-disruptive-technologies-in-defence

TRITHART, A. 2022. Disinformation against UN Peacekeeping Operations. International Peace Institute, November 2022. Available at: https://www.ipinst.org/wp-content/uploads/2022/11/2212_Disinformation-against-UN-Peacekeeping-Ops.pdf

United Nations Peacekeeping. 2025a. Actions for Peacekeeping+. Available at: https://peacekeeping.un.org/en/action-peacekeeping

United Nations Peacekeeping. 2025b. Data. Available at: https://peacekeeping.un.org/en/data].

United Nations Peacekeeping. 2025c. What Peacekeeping Does. Available at: https://peacekeeping.un.org/en

United Nations. General Assembly. 2021. *Disinformation and freedom of opinion and expression* Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan. 2021. Available at: https://docs.un.org/en/A/HRC/47/25

United Nations. General Assembly. 2023. *Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training.* 2023. Available at: https://webarchive.unesco.org/web/20230926213448/https://en.unesco.org/fightfakenews

VEUGER, J. 2018. Trust in a viable real estate economy with disruption and blockchain. In: *Facilities*, 2018, Vol. 36, No. 1-2. 103-120. Available at: https://doi.org/10.1108/F-11-2017-0106

VINCIĆ, N. 2021. *The Future of Warfare: Security Implications of Emerging and Disruptive Technologies (EDTs),* 2021. Available at: https://natoassociation.ca/the-future-of-warfare-security-implications-of-emerging-and-disruptive-technologies-edts/

Assist.prof. Elisabeta-Emilia HALMAGHI, PhD
Faculty of Military Management, “Nicolae Bălcescu” Land Forces Academy
Revolutiei Street No. 3-5
550170 – Sibiu, Romania
emmahalmaghi@gmail.com

LTC Assoc.prof. Alin CÎRDEI, PhD
Faculty of Military Sciences, “Nicolae Bălcescu” Land Forces Academy
Revolutiei Street No. 3-5
550170 – Sibiu, Romania
cirdei_alin@yahoo.com

Assist.prof. Ileana-Gentilia METEA, PhD
Faculty of Military Sciences, “Nicolae Bălcescu” Land Forces Academy
Revolutiei Street No. 3-5
550170 – Sibiu, Romania
meteaileana@yahoo.de

COL.eng. Daniela CĂRUȚAȘU, PhD
“Nicolae Bălcescu” Land Forces Academy
Revolutiei Street No. 3-5
550170 – Sibiu, Romania
d.carutasu@yahoo.com

DOI: https://doi.org/10.52651/vr.a.2025.3.70-87

VOJENSKÉ REFLEXIE
ISSN: 1336-9202 (online)
2025, Number 3, Page 70-87

THE RECRUITMENT OF YOUTH INTO TERRORIST GROUPS: PSYCHOLOGICAL, SOCIAL AND SECURITY ASPECTS

Peter GAŽO, Soňa ŠROBÁROVÁ, Lubomír BELAN, Mária MARTINSKÁ

ARTICLE HISTORY

Submitted: *19.09.2025*
Accepted: *27.11.2025*
Published: *31.12.2025*

ABSTRACT

The recruitment of youth into terrorist groups represents a multidimensional security challenge that integrates psychological vulnerability, social instability and the increasing influence of digital environments. Based on the established radicalisation frameworks (Moghaddam, Kruglanski, Borum, Wiktorowicz), this article examines the complex mechanisms through which adolescents become susceptible to extremist narratives and recruitment strategies. The analysis introduces an Integrated Multidimensional Model of Youth Radicalisation (IMMRM), which conceptualises radicalisation as the interaction of unmet psychological needs for identity and significance, weakened family and community ties, and exposure to algorithmically reinforced online spaces that normalise extremist content. The study identifies the key risk factors specific to Generation Z and highlights how digital platforms, emotional manipulation and online grooming accelerate the recruitment process. The findings underline the need for systemic, evidence-based prevention combining psychological support, educational interventions, digital literacy and early detection of risk signals. The article advances the argument that an effective safeguarding framework against youth radicalisation and terrorist recruitment must be grounded in a coordinated, interdisciplinary, and technologically informed approach.

KEYWORDS

recruitment; youth; terrorism; radicalization; online recruitment

INTRODUCTION

The recruitment of young people into terrorist groups is becoming increasingly topical and more complex security issue. The dynamics of globalisation, the rise of digital technologies and the spread of social media have significantly influenced the ways in which terrorist organisations reach out to potential members. In this context, young people appear to be an extremely vulnerable group – they are in the process of forming their identity, searching for their place in society, and are often exposed to various forms of social and psychological pressure.

Terrorist groups deliberately exploit this vulnerability and apply sophisticated recruitment strategies – from ideological propaganda to psychological manipulation (known as grooming). The aim of these strategies is to secure long-term loyalty and create a network of followers and potential perpetrators of violent acts.

This phenomenon threatens not only individuals, but also broader social stability and national security. The aim of this article is to present the recruitment of youth as a multidimensional phenomenon and to highlight its deeper psychological, social and technological roots. The theoretical part will explain the concept of radicalisation as a precursor to involvement in extremist structures and analyse the main factors that influence the vulnerability of young people.

The aim of this article is to present youth recruitment as a multidimensional phenomenon and to analyses its deeper psychological, social, and technological roots. The theoretical part will explain in detail the concept of radicalization as a precursor to involvement in extremist structures, followed by an analysis of the main factors that influence the increased vulnerability of youth to these influences. In writing this article, the authors used scientific methods – analysis, synthesis, analytical comparison, deduction, and abstraction. In the concluding section of the article, the authors reflect on the use of the analysed findings on the issue in question and present proposals for possible practical solutions.

1 THEORETICAL FOUNDATIONS OF THE PROBLEM

Terrorism is a complex social phenomenon, the definition of which often varies depending on the cultural, political and historical context. Etymologically, the term "terrorism" comes from the Latin word "Terrere", which means to threaten, frighten or cause terror[1]. In the broadest sense, terrorism can be defined as the organised use of violence to instil fear and achieve political goals. The essence of terrorist activities is the illegal use of force against individuals or property with the intention of intimidating the government, the civilian population or a specific part of it, and fulfilling political, religious or social ambitions. Terrorism can also be understood as the use of threats or violence directed against the constitutional order of states, whereby the states themselves are not its direct victims.

The victims of terrorism can be anonymous persons, specific individuals or strategic and cultural objects. A key aspect of terrorist acts is the intention to cause fear and intimidate the wider society through attacks on innocent victims. In international law and political discussions, terrorism is often understood as asymmetric warfare, where non-state

[1] Horror is a feeling of fear, anxiety, and dread. It refers to a state in which someone is exposed to something extremely negative, dangerous, or frightening. It can refer to real events, but also to imaginary ideas. Horror encompasses fear, dread, despair, and terror. The context in which the word horror is used is often related to danger, violence, tragedy, or supernatural phenomena.

actors attack civilian targets in order to achieve a psychological effect on the public and political leaders. According to the UN definition, terrorism is *"any act intended to cause death or serious injury to civilians or unarmed persons with the aim of intimidating the population or compelling a government or international organisation to perform or refrain from performing any act"*. (Kubrina, 2018)

There are various definitions of terrorism in Slovakia. The Small Slovak Encyclopaedia from 1993 defines terrorism as "*methods of gross intimidation of political opponents through the threat of violence*" (Kulasik, 2002). The Security Policy Dictionary understands terrorism as "*politically motivated acts, including bombings, kidnappings and other violent acts aimed at intimidating political opponents, influencing public opinion or exerting pressure on individuals or groups of the population*" (Kulasik, 2002). Currently, there is no single or universal definition of terrorism. Some critics argue that it is a *"rhetorical weapon"* to eliminate opponents of the established order. According to Brzobohatý, the perception of terrorism is very vague, ambiguous and subjective. This term evokes various associations, which makes it difficult to analyse this phenomenon. (Smolík, 2020)

1.1 Recruitment and enlistment

The recruitment and enlistment in the context of terrorism represent a key process through which terrorist organisations acquire new members who subsequently become involved in their activities, including terrorist attacks. This process has various stages, starting with approaching potential recruits, continuing with persuasion, and ending with the actual acceptance of the individual into the organisation. It is important to distinguish between recruitment, which focuses on finding potential candidates, and enlistment, which involves their active integration into the organisation. The main objective of the recruitment process is to maintain and expand the membership base of a terrorist organisation, which is essential for its long-term functioning. Terrorist organisations often target individuals with weak social ties, such as young people, individuals with strongly radical or fundamentalist views, lonely individuals, or mentally unstable people. These individuals are considered more susceptible to manipulation and acceptance of radical ideologies.

The recruitment process currently makes extensive use of modern technologies, particularly the internet and social media. These platforms provide anonymity and are ideal tools for spreading radical ideas and recruiting new members. Terrorist organisations use the internet to disseminate propaganda, videos and ideological materials, thereby reaching a wider audience. The internet allows not only for the passive reception and sharing of this information, but also for active participation in communities that support radical views. Recruiters use various psychological techniques, including emotional manipulation and offering simple solutions to complex global problems, which contributes to the radicalisation of individuals.

The recruitment process often targets factors such as the search for identity, the desire for a higher meaning in life, or the need for uniqueness that membership in a terrorist organisation can seemingly offer. The persuasion process is often sophisticated and involves not only verbal communication but also non-verbal techniques such as eye contact or gestures, which have a strong emotional and ideological impact on individuals. An important aspect of the recruitment process is the ability of terrorist organisations to use the media, including reports of terrorist attacks, which can elicit sympathy or interest in the ideology among some people. Some organisations also use preachers who spread extremist ideologies in various communities, such as schools or religious centres, thereby directly addressing potential new members. (Lichner et al, 2018)

1.2 The Psychological and digital determinants of youth radicalization

The process of youth radicalisation cannot be explained in isolation as an ideological or political phenomenon, but as the result of complex interactions between psychological, social and digital factors. Due to their developmental characteristics, young people are more susceptible to adopting extreme ideas that offer them a sense of identity, meaning and belonging. According to the "Three Pillars of Radicalisation" model (Kruglanski, Bélanger & Gunaratna, 2019), this process is based on needs, narratives and social networks, which together form a framework in which radical attitudes are internalised.

The psychological determinants

From a psychological perspective, radicalisation is closely linked to young people's need to find meaning, significance and belonging. Adolescents face various developmental challenges – the search for identity, separation from parental authority and the pursuit of autonomy make them vulnerable to the offers of groups that provide them with clear answers and a sense of certainty (Smolík, 2020). Terrorist and extremist organisations exploit these psychological needs by offring a narrative of a 'higher purpose', heroism or revenge, which resonates particularly with individuals with low self-esteem or frustration with their social status. (Lichner et al, 2018)

Kruglanski (2019) describes the concept of the "need for significance", which can lead to radicalisation in situations where an individual experiences feelings of humiliation, rejection or loss of dignity. Combined with a collective narrative that legitimises violence as a "morally justified act", this creates a psychological basis for extremist behaviour. According to Moghaddam (2005), radicalisation proceeds as a "psychological staircase to terrorism", where individuals gradually move from perceiving injustice to believing that violence is the only effective solution.

Group identity is also an important psychological factor. The process of socialisation in radical communities reinforces so-called ingroup-outgroup thinking ("us" versus "them"), which reduces empathy towards others and increases tolerance for violence. Cognitive dissonance (Festinger, 1957) also plays a significant role, leading individuals to rationalise their actions in line with their new beliefs. Young people in such an environment become convinced of their own moral superiority and perceive violence as a legitimate means of protecting "justice" or "faith".

The digital determinants

The digital environment is a key factor that fundamentally changes the nature of radicalisation. The internet and social networks create virtual communities in which radical ideas spread quickly, anonymously and without territorial boundaries (Conway, Scrivens & Macnair, 2019). At the same time, social media algorithms promote the phenomenon of echo chambers and filter bubbles, which reduce contact with different opinions and reinforce the belief in the "truth" of radical ideologies.

The recruitment strategies of terrorist groups in the online environment often use emotional manipulation, personalised propaganda and grooming, i.e. building trust between the recruiter and the young person. The targeted use of visual and game-oriented elements – so-called "gamification of radicalisation" – makes it possible to transform ideological content into an attractive experience. Videos, memes and interactive applications are designed to evoke a sense of adventure and social recognition.

Cyber anonymity also plays an important role. Platforms such as Telegram, Signal and Rocket Chat allow the creation of closed groups where young people can become radicalised beyond the reach of the authorities. These spaces often serve as so-called incubators of extremism – environments in which extremist identities and collective narratives are formed.

From a psychological point of view, it is dangerous that young users often lack sufficiently developed media and critical skills, which makes them susceptible to disinformation, conspiracy theories and propaganda. The inability to distinguish credible sources from manipulative ones increases the risk of accepting extreme attitudes as "authentic truths".

The synergistic effect of psychology and technology

The psychological and digital determinants of radicalisation work synergistically – young people's psychological needs for identity, meaning and belonging find ideal conditions for fulfilment in the online environment through extremist communities. The digital space is thus not only a platform for spreading propaganda, but also a psychosocial space for the formation of a new identity that can become entrenched in violent forms of behaviour.

Understanding these determinants is key to developing effective prevention strategies. Interventions should aim not only to prevent access to radical content, but also to strengthen the mental resilience, critical thinking and social integration of young people. The combination of psychological knowledge and digital security provides a modern framework for responding effectively to the changing forms of radicalisation in the 21st century.

1.3 Radicalization as a precursor to terrorism

Radicalisation is a process that usually precedes recruitment and may or may not lead to violent activities. In the context of the internet and social media, this process plays a crucial role, as the digital environment allows for the faster spread of radical ideologies and the formation of closed groups with shared beliefs. Unlike recruitment itself, radicalisation is a long-term process during which opinions and attitudes that can lead to violent acts. This process can take place individually or collectively – within groups, communities or wider society . (Lichner et al, 2018)

According to Koomen and Plight's definition, radicalisation is "*the development of opinions, beliefs and ideas that lead individuals to ultimately accept the commission of a terrorist act"* (Koomen and Plight, 2016). In this context, social media plays a key role, as it facilitates interaction between already radicalised individuals and those who are susceptible to adopting extreme views.

Radicalization in the online environment can be reinforced by several factors, such as:

1. Developmental factors: Adolescence is characterised by experimentation and the search for one's own identity, which can lead to the rejection of the values of parents and society. Radical attitudes may appear attractive because they differ from traditional norms (Borum, 2011).
2. Social factors: A lack of a sense of belonging, growing up in broken families, or social exclusion can lead to seeking refuge in extremist groups that provide a sense of "belonging" and compensate for the need to be part of a community (Mølmen, M. H., & Ravndal, J. A., 2021; Ranthorp, M., & Meines, M. R., 2024).
3. Technological factors: The current generation is growing up in an environment of modern technology and social media, which gives them access to a wide range of information, but they often lack the ability to critically evaluate this information, which can contribute to their susceptibility to manipulation and the acceptance of radical ideas. (Conway, 2017, Žúborová, V., Borárosová, I., & Vašečka, M., 2019; Binder, J. F., & Kenyon, J., 2022).
4. Economic and political factors: Young people live in a time of economic and political uncertainty, which can lead to concerns about national identity and social stability.
5. Personal experiences: Personal experiences of social exclusion, aggressive upbringing, experiences of violence, or frustration with one's social status can contribute to the emergence of extremism. (Koomen & Pligt, 2016).

Acts of terrorism do not usually appear suddenly and without warning. They are almost always preceded by a process of radicalisation. The process of radicalisation itself does not necessarily lead to terrorist acts, but it represents a phase in which it is possible to prevent the further development of terrorist acts or to reverse them completely. Radicalism can be seen as the final stage of the process of radicalisation. This process can take place at the individual level (intrapersonal radicalisation), but also within a group, community or subculture. Radicalisation can also affect society as a whole. Radicalisation processes are present in all forms of terrorism, whether political, religious, separatist, environmental or ethno-nationalist (Borum, R., 2011).

1.4 Young people as a target group

Young people, especially during adolescence, are considered a high-risk target group that is prone to accepting simplified and often distorted views on complex social issues. This age group is characterised by developmental and psychological factors that significantly influence the formation of young people's identities and attitudes. Sympathy for extremism can be manifested in various ways among adolescents, such as violent acts against certain social groups, participation in illegal events, wearing prohibited symbols or founding extremist organisations.

In addition to external manifestations of behaviour, extremism also influences young people's overall view of the world and their way of thinking. Adolescents with extremist tendencies often have unconventional views on social issues and seek simple solutions to complex questions, which can lead to radicalisation.

There are several reasons why young people are more susceptible to such attitudes. The developmental and social psychology explains that adolescence is a period of experimentation and a search for one's own identity, which can lead to a rejection of the values of parents and society. In this context, radical attitudes may appear attractive because they differ from traditional norms.

Another important factor is a lack of a sense of belonging. Young people who grow up in broken families or experience social exclusion may be prone to seeking refuge in extremist groups that give them a sense of "belonging" and compensate for their need to be part of a community. The current generation of adolescents, referred to as Generation – Z or the digital generation, is growing up in an environment of modern technology and social media, which gives them access to a wide range of information. However, they often lack the skills to critically evaluate this information, which increases their vulnerability to manipulation and accepting radical ideas.

Young people also live in a time of economic and political uncertainty, which can lead to concerns about national identity and social stability. Factors that can contribute to the emergence of extremism include personal experience of social exclusion, aggressive upbringing, experiences of violence or frustration with one's own social status. According to the modernisation concept, the younger generation is often considered to be victims of rapid social change, which can lead to disorientation and frustration. This process can influence their propensity for radical behaviour.

An interesting finding is that supporters of extremism include young people who have stable jobs, not just the unemployed. This suggests that the causes of extremism are not only social and economic, but also psychological and cultural. Adolescents who join extremist groups often organise public events such as concerts and marches and contribute to websites with extremist themes. At the same time, there are also sympathisers who identify with these groups only in their opinions or through external manifestations, such as wearing extremist symbols, but do not participate in active activities. (Koomen & Pligt, 2016; Ondrejkovič, 1994, 2003, Lichner et al, 2018)

2 POSSIBLE SOLUTIONS AND TECHNOLOGICAL PERSPECTIVES

The issue of recruiting young people into terrorist groups requires a comprehensive and multidisciplinary approach to solving it. Based on the theoretical principles identified in the previous section, we can propose several strategies and measures that could contribute to the prevention and resolution of this serious security problem.

Given that young people are particularly vulnerable to radicalisation due to developmental and psychological factors, it is necessary to focus on preventive measures that strengthen young people's resilience to extremist ideologies. One key aspect is to promote the development of critical thinking, which will enable young people to better evaluate the information they encounter online. Strengthening identity and a sense of belonging to society is also an important element of prevention.

As the analysis shows, young people who suffer from a lack of belonging are more likely to seek refuge in extremist groups. It is therefore essential to create opportunities for meaningful youth participation in social life and to support them in building positive social ties. Psychological support and counselling for young people who are going through crisis situations or experiencing frustration can be another effective prevention tool. These services should be easily accessible and focused on helping young people cope with the emotional and social challenges that can contribute to radicalisation. (Binder, Kenyon, 2022)

Education plays a key role in preventing radicalisation and the recruitment of young people into terrorist groups. It is necessary to implement educational programmes focused on developing media and digital literacy, which will enable young people to better recognise the manipulative techniques used in the online space.

Schools should also include topics related to extremism, terrorism and radicalisation in their curricula, with an emphasis on critical analysis of these phenomena and their social impact. Such educational initiatives should be tailored to the age of the students and should help them understand the complexity of social issues, thereby reducing the likelihood of accepting simplistic and extremist solutions. Raising awareness about the recruitment mechanisms and techniques used by terrorist organisations can also contribute to the prevention of radicalisation. This includes information campaigns targeting young people, their parents and educators, explaining how terrorist organisations specifically target young people and what psychological techniques they use to manipulate them. (Conway, 2017, Žúborová, Borárosová, Vašečka, 2019; Binder, Kenyon, 2022)

As the internet and social media are the main platforms for spreading extremist ideologies and recruiting new members, regulating the online space is an essential part of addressing this problem. This includes monitoring and removing extremist content, as well as identifying and disrupting recruitment activities in the online space. Cooperation with social media operators and technology companies is key to developing and implementing effective strategies to identify and limit the spread of radical content. At the same time, it is important to ensure that these measures respect fundamental rights and freedoms, including freedom of expression.

Given the global nature of terrorism and terrorist organisations, international cooperation is an essential part of effectively addressing the problem of youth recruitment. This cooperation should include the exchange of information, best practices and experiences between countries and international organisations. Coordinated efforts to combat terrorist propaganda and recruitment activities in the online space can increase the effectiveness of preventive measures. At the same time, it is important to support research into radicalisation and youth recruitment, which will contribute to a better understanding of these processes and the development of more effective countermeasures. (Conway, 2017, Žúborová, Borárosová, Vašečka, 2019; Binder, Kenyon, 2022)

3 MULTIDIMENSIONAL ANALYSIS OF PSYCHOLOGICAL, SOCIAL, AND DIGITAL DETERMINANTS OF ADOLESCENT RADICALIZATION

The radicalization of adolescents is the result of an interplay between individual psychological needs, the social environment, and the specific characteristics of the digital world. To gain a deeper understanding of this process, it is appropriate to draw on several established models of radicalization and integrate them into a synthetic framework adapted to the Slovak context.

This analytical section is based on the “psychological staircase to terrorism” model (Moghaddam, 2005), the “Three Pillars of Radicalization” concept (Kruglanski, Bélanger & Gunaratna, 2019), Borum’s four-stage model of radicalization (2011), and Wiktorowicz’s theory of joining extremist groups (2005).

The following table provides a schematic comparison of the key characteristics of each model and their relevance to adolescent radicalization (table.1).

Table 1 At-Risk vs. Resilient Adolescents

Domain	**At-risk adolescent (higher susceptibility to radicalization)**	**Resilient adolescent (higher resistance to radicalization)**
Need for meaning and identity	Strongly felt need to "be someone," feelings of insignificance, often seeks identity outside family and school	Relatively stable sense of self-worth; identity supported by family, school and extracurricular activities
Self-esteem	Low self-esteem, frequent self-devaluation or, conversely, fragile "inflated" confidence	Adequate self-esteem; ability to acknowledge weaknesses without excessive shame
Identity	Conflicted, fragmented identity; sense of "I don't belong anywhere"	Integrated identity; sense of belonging to multiple positive groups (family, school, clubs)
Emotion regulation	Impulsivity; difficulty managing anger, frustration, and shame	Ability to delay reactions; use of adaptive emotion regulation strategies
Perception of injustice	Perceives the world as deeply unfair; feelings of victimhood; blaming specific groups ("them")	Differentiates between personal adversity and systemic injustice; open to multiple explanations
Family relationships	Weak emotional connection, conflict, distrust or disinterest; lack of support	Relatively stable, supportive relationships; space for dialogue and sharing problems
School environment	Experiences of bullying, academic failure, frequent criticism, lack of recognition	Minimal or adequately addressed bullying; experiences success and recognition (academic/extracurricular)
Peer relationships	Often marginal member of peer groups or part of "protest" subcultures; contact with radicalized peers	Accepted by peer groups that promote prosocial values
Online behavior	High amount of time in online environments with polarized or extremist content; anonymous identities	Balanced online activity; exposure to diverse content; basic media literacy
Personality traits	Higher sensation-seeking, impulsivity, neuroticism; low frustration tolerance	Higher conscientiousness, emotional stability, openness to dialogue; higher frustration tolerance
Coping and stress response	Predominantly maladaptive strategies (escape into online world, aggression, substance misuse)	Adaptive strategies (seeking help, conversation, sports, creative activities)
Attitude toward authority and norms	Strong opposition; rigid "anti-system" views; black-and-white worldview	Critical thinking combined with ability to engage in dialogue and accept plurality of viewpoints

Source: own processing - modified according to Kruglanski, Bélanger & Gunaratna, 2019

These models complement one another: Moghaddam highlights the vertical process of escalation, Kruglanski emphasizes the need for significance and social networks, Borum analyzes cognitive frames, and Wiktorowicz describes the mechanisms of group entry. When applied to the Slovak Gen Z context, it is essential to add the digital dimension (social media, algorithms, online communities).

Based on the theoretical approaches analyzed, an Integrated Multidimensional Model of Adolescent Radicalization (IMMRM) can be proposed for the needs of security and prevention practice in Slovakia. The model draws from the psychological concept of the need for significance (Kruglanski et al., 2019), the dynamics of frustration and perceived injustice (Moghaddam, 2005; Borum, 2011), the theory of social bonds in joining extremist groups (Wiktorowicz, 2005), and the influence of the digital environment on the formation of extremist identities (Conway, Scrivens & Macnair, 2019). It assumes three interconnected dimensions – psychological, social, and digital.

The psychological dimension includes the need for significance, recognition, and identity (Kruglanski et al., 2019), experiences of injustice, humiliation, or marginalization (Moghaddam, 2005; Borum, 2011), and low self-esteem or identity conflict typical of adolescence.

The social dimension is based on the assumption that the risk of radicalization increases in dysfunctional family environments, in situations marked by conflict, neglect, or weak emotional attachment. The school environment also plays a significant role — especially experiences of bullying, academic failure, or lack of support. Peer groups and local subcultures are also important, as they may normalize extremist patterns of behavior. The radicalization process accelerates in cases of personal contact with radicalized individuals or recruiters (Wiktorowicz, 2005).

The digital dimension reflects the specifics of the online environment in which adolescents spend a substantial amount of time. Dominant features include radicalizing narratives and visual propaganda circulated through social media (Conway et al., 2019), as well as the effects of echo chambers and filter bubbles, which reinforce one-sided perspectives. Online grooming, the gamification of radicalization, memes, interactive elements, and the anonymity of the internet — which enables young people to experiment with identity without immediate consequences — also play an important role.

The IMMRM model assumes that the risk of radicalization increases significantly when these three dimensions overlap synergistically — when an adolescent with an unfulfilled psychological need for significance (P) lives in a socially unstable environment (S) and simultaneously operates within digital communities that normalize radical content (D).

4 RISK FACTORS FOR RADICALIZATION AMONG GENERATION Z

Within the IMMRM framework, several demonstrable risk factors can be identified for Generation Z. Psychological risks are primarily associated with an intensified need to stand out and feel “exceptional,” heightened sensitivity to humiliation or exclusion, feelings of helplessness and frustration, as well as a higher prevalence of anxiety and depressive symptoms. These conditions reduce a young person’s ability to process complex information and increase susceptibility to black-and-white thinking (Kruglanski et al., 2019; Moghaddam, 2005).

Social factors include weakened family bonds and a conflictual home environment, experiences of bullying (both offline and online), stigmatization, exclusion from peer groups, or living in communities with low social cohesion. Risk is further increased by contact with peers who sympathize with extremist ideologies or who are actively involved in radicalized groups (Borum, 2011; Wiktorowicz, 2005).

Digital risks relate to excessive time spent in closed online communities (gaming environments, radicalized forums, Discord/Telegram groups), repeated exposure to hateful or conspiratorial content, and interaction with radicalizing narratives presented in visually appealing forms (memes, music videos, “heroic” clips). Low media and digital literacy also plays a significant role, as it reduces the ability to distinguish manipulation from factual information (Conway et al., 2019).

Including the IMMRM in the analytical section of the article allows theoretical concepts to be linked with practical recommendations for prevention. The model also provides a foundation for developing targeted educational programs, strengthening digital literacy, and enhancing psychosocial support for at-risk adolescent groups—representing key tools for preventing radicalization in the context of the Slovak Republic.

CONCLUSION

Based on the multidimensional analysis, it can be concluded that the radicalization of adolescents in the Slovak context does not arise in isolation but is the result of the synergistic interaction of psychological, social, and digital determinants. The Integrated Multidimensional Model of Adolescent Radicalization (IMMRM) demonstrates that the risk of radicalization increases significantly especially when an adolescent simultaneously experiences an unmet need for identity and significance, weakened family and school bonds, and intensive exposure to online environments that normalize extremist narratives.

The analysis indicates that Generation Z is substantially more vulnerable than previous generations to online radicalization mechanisms, particularly due to phenomena such as echo chambers, algorithmic content filtering, visually appealing forms of propaganda, and the gamification of extremist ideologies. Psychological risk factors (low self-esteem, the need to stand out, sensitivity to humiliation), social circumstances (bullying, social exclusion, weak family ties), and digital dynamics (anonymity, closed forums, conspiratorial narratives) mutually reinforce one another.

Terrorism is a complex social phenomenon involving the use or threat of violence to achieve political, religious, or ideological objectives. Although definitions vary depending on cultural and political contexts, the core element is the intent to instill fear and intimidate society.

Recruitment and enlistment represent key processes through which terrorist organizations acquire new members. These processes include several stages, from identifying potential candidates to their active integration into the organization. The internet and social media significantly facilitate these processes by providing a platform for disseminating extremist ideologies and enabling terrorist organizations to reach a wider audience.

Youth are particularly vulnerable to radicalization and recruitment into terrorist organizations. This vulnerability is shaped by developmental and psychological factors, as well as social and cultural influences. Young people in adolescence seek identity and a place in society, which may make them more susceptible to extremist ideologies. Factors such as a lack of belonging, personal experiences of social exclusion, or frustration with one's social status can contribute to increased vulnerability.

In conclusion, the IMMRM provides a framework that is particularly suitable for the Slovak environment, as it integrates internationally established models of radicalization (Moghaddam, Kruglanski, Borum, Wiktorowicz) while simultaneously reflecting the rapidly changing digital contexts in which Slovak youth operate. This framework enables better targeting of preventive measures, identification of at-risk groups, and the design of interventions that respond to the needs of adolescents in the contemporary information environment.

Recommendations for practice

Based on the synthetic IMMRM model, several specific recommendations can be identified that complement previous proposals and focus on the three key dimensions of radicalization. These recommendations include the implementation of comprehensive prevention programs aimed at strengthening young people's resilience to radicalization. Such programs should include the development of critical thinking, media literacy, and social skills.

Terrorism is a complex social phenomenon that involves the use of violence or the threat of violence to achieve political, religious or ideological goals. Its definitions may vary depending on the cultural and political context, but the basic element is the intention to cause fear and intimidate society. Recruitment and enlistment are key processes through which terrorist organisations gain new members. These processes involve various stages, from approaching potential candidates to actively integrating them into the organisation. The internet and social media significantly facilitate these processes, as they provide a platform for the dissemination of extremist ideologies and enable terrorist organisations to reach a wider audience

The following recommendations correspond to the psychological, social, digital, research, and legislative dimensions of prevention:

Recommendations in the Psychological Dimension:

- Establish systematic programs focused on building adolescents’ self-esteem, resilience, and identity, particularly within school settings.
- Strengthen the availability of psychological services, crisis intervention, and preventive programs in schools and communities.
- Implement programs aimed at reducing feelings of isolation, frustration, or shame, which, according to Moghaddam and Kruglanski, represent key triggers in radicalization processes.

Recommendations in the Social Dimension:

- Strengthen family-oriented interventions—parental education, counseling services, and programs aimed at improving family relationships, which reduce adolescents’ vulnerability.
- Introduce school-based prevention programs addressing bullying, social exclusion, and stigmatization, as these factors are among the main entry points into radicalization according to Borum and Wiktorowicz.
- Support community-based activities for youth (sports, arts, volunteering) that enhance a sense of belonging and serve as protection against entry into high-risk peer groups.

Recommendations in the Digital Dimension:

- Strengthen digital and media literacy, including the ability to identify manipulative content, conspiracy narratives, and radicalization strategies.
- Create educational modules in schools and communities about the risks of online radicalization, gamified recruitment strategies, and the dangers of anonymous online spaces.
- Improve monitoring of high-risk platforms in cooperation with state and security institutions, technology companies, and social media providers.

Recommendations for Research and Security Practice:

- Develop a national framework for monitoring radicalization trends among adolescents in the online environment (SOCMINT/OSINT).
- Support interdisciplinary research combining psychology, sociology, security studies, and digital analytics.
- Strengthen the training of professionals (social workers, psychologists, teachers, police officers) in the early detection of radicalization signals.

- Implement evidence-based procedures inspired by international best practices (Aarhus Model, Hayat, EXIT programs) and adapt them to the Slovak context.

Recommendations for Legislation and State Policy:

- Update national strategic documents on the prevention of radicalization to reflect the dynamics of the digital environment.
- Introduce standardized protocols for working with radicalized adolescents, similar to existing procedures for violent behavior or addictions.
- Support security policies aimed at protecting minors in the online environment, particularly on closed platforms (Telegram, Discord, encrypted chats).

Challenges for the future

Despite the proposed solutions, there are several challenges that will need to be addressed in the future:

1. The rapid development of technology and communication platforms, which can provide terrorist organisations with new tools to spread their ideology and recruit new members. It is necessary to ensure that preventive measures keep pace with these developments.
2. Balancing between the need to regulate the online space and the respect for fundamental rights and freedoms, including freedom of expression. It is important to find a balance that allows for effective prevention of radicalisation without unduly restricting civil liberties.
3. The need to address the root causes of radicalisation, including socio-economic factors, political marginalisation and cultural conflicts. These deeper problems require long-term and comprehensive solutions that go beyond security measures.
4. The vulnerability of new generations of young people to radicalisation in the context of a changing global situation and new social challenges. Preventive strategies need to be continuously updated and adapted to the specific needs and characteristics of new generations .
5. The need to evaluate the effectiveness of preventive measures and interventions. It is important to develop methods for measuring the success of these measures and to use the knowledge gained to continuously improve them.

In conclusion, we can say that the issue of recruiting young people into terrorist groups is a complex security problem that requires a coordinated approach involving preventive, educational, social and regulatory measures. Only through a comprehensive approach and international cooperation can we effectively protect young people from radicalisation and recruitment into terrorist organisations and thus ensure a stable and secure society. In summary, the issue of youth recruitment into terrorist organizations represents a complex security challenge that requires a coordinated approach involving preventive, educational, social, and regulatory measures. The analysis confirms that radicalization prevention must be multidimensional and responsive to the psychological, social, and digital determinants that shape the behavior of Generation Z. Effective protection of young people from radicalization therefore requires systematic support from schools, families, and communities, which play a key role in building resilience.

An important protective factor is the development of digital literacy and the ability to critically engage with online content, as most radicalization processes today occur within social media and multimedia platforms. The radicalization of adolescents is not the result of simple ideological indoctrination but rather a combination of developmental identity needs, experiences of frustration, and the intense influence of online environments that normalize extremist narratives.

This implies that preventive measures must be continuous, adaptive, and based on real-time monitoring of trends in the digital space. Only through such a comprehensive and long-term coordinated approach—supported by international cooperation and the sharing of best practices—can we effectively protect young people from radicalization and recruitment into terrorist organizations while strengthening the stability and security of society.

REFERENCES

BINDER, J. F., & KENYON, J. (2022). Terrorism and the internet: How dangerous is online radicalization?. Frontiers in Psychology, 13, 997390. DOI: https://doi.org/10.3389/fpsyg.2022.997390

BORUM, R. (2011). Radicalization into Violent Extremism I: A Review of Social Science Theories. Journal of Strategic Security, 4(4), 7–36. DOI: https://doi.org/10.5038/1944-0472.4.4.1

CONWAY, M. (2017). *Determining the role of the internet in violent extremist processes*. *Handbook of the criminology of terrorism*. DOI: https://doi.org/10.4324/9781315692029-8

CONWAY M., SCRIVENS R., MACNAIR L. (2019). Right-Wing Extremists' Persistence Online Presence: History And Contemporary Trend. The Hauge: International Center for Counter-Terrorism. - Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends History and Contemporary Trends on JSTOR

CONWAY, M., SCRIVENS, R., & MACNAIR, L. (2019). Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends. ICCT Policy Brief. DOI: 10.19165/2019.3.12; ISSN: 2468-0486. icct.nl

EROĞLU, Zehra Can. Children recruiting and exploiting by terrorist groups. Defence Against Terrorism Review, 2022, 16: 109-129.

EURÓPSKA KOMISIA. (n.d). Newsbrief. European Media Monitor. https://emm.newsbrief.eu/NewsBrief/alertedition/en/TerroristAttack.html

LICHNER, V., ŠLOSÁR, D., ŠIŇANSKÁ, K., TÓTHOVÁ, L. PLAVNICKÁ, J., HOVANOVÁ, M., VASIĽOVÁ, V., ŽIAKOVÁ, T., KAHAN, J., ŠIMKO, J. (2018) Extrémizmus a radikalizácia v sociálnych kontextoch. Košice 2018. ISBN 978-80-8152-659-6

FESTINGER, L. (1957). A Theory of Cognitive Dissonance. Stanford University Press. ISBN-13: 978-0804709118; ISBN-10: 0804709114. https://doi.org/10.1515/9781503620766

KOOMEN, W. ang PLIGT, J. van der. (2016) The Psychology of radicalization and terrorism. London: Routledge, Taylor & Francis Group, 2016. ISBN 978-1-84872-441-9.

KRUGLANSKI, A. W., BÉLANGER, J. J., & GUNARATNA, R. (2019). The Three Pillars of Radicalization: Needs, Narratives, and Networks. Oxford University Press. ISBN-13: 978-0190851125; DOI: https://doi.org/10.1093/oso/9780190851125.001.0001

KUBRINA, E. 2018. Metody verbování mládeže a propagandistická činnost teroristických skupin, inspirovaných ideologií saláfitského džihádismu [diplomová práca]. Praha: Univerzita Karlova [s. n.], 2018. 105 s., str. 28-30

KULAŠIK, Peter. Slovník bezpečnostných vzťahov. 2., doplnené a upr. vyd. Bratislava: Smaragd, 2002. ISBN 80-89063-08-X.

Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky. Slovensko v rámci boja proti terorizmu. Online. MZV.sk. 2024. Dostupné z: https://doi.org/https://www.mzv.sk/diplomacia/bezpecnostna-politika/slovensko-v-ramciboja-proti-terorizmu [cit. 2025-10-03].

MOGHADDAM, F. M. (2005). The Staircase to Terrorism: A Psychological Exploration. American Psychologist, 60(2), 161–169. DOI: https://doi.org/10.1037/0003-066X.60.2.161

MØLMEN, M. H., & RAVNDAL, J. A. (2021). *Risk factors for internet-facilitated radicalisation: A systematic review*. Journal of European Crime Policy and Research.

NEČAS, P. a J. UŠIAK, 2010. Nový prístup k bezpečnosti štátu na začiatku 21. storočia. Liptovský Mikuláš: Akadémia ozbrojených síl generála Milana Rastislava Štefánika. ISBN 978-80-8040-401-7. 167 s.

ONDREJKOVIČ, P. (1994) *Základy sociológie mládeže. Bratislava:* Iuventa, 1994. ISBN: 80-8517-244-5, s.84

ONDREJKOVIČ, P. (2003) *Základy sociológie mládeže - mládež v zrkadle sociológie výchovy a mládeže.* Nitra : Fakulta sociálnych vied UKF, 2003, ISBN: 80-8050-658-2. str.124-131.

SMOLÍK, Josef. Psychologie terorismu a radikalizace: jak se z beránků stávají vlci. Vydání: první. V Brně: Mendelova univerzita, 2020. ISBN 978-80-7509-723-1, str. 18

RANTHORP, M., & MEINES, M. R. (2024). *The root causes of violent extremism*. Radicalisation Awareness Network (RAN), European Commission

WIKTOROWICZ, Q. (2005). Radical Islam Rising: Muslim Extremism in the West. Lanham: Rowman & Littlefield. ISBN: 978-0742536418 DOI: https://doi.org/10.5771/9781461641711

ŽÚBOROVÁ, V., BORÁROSOVÁ, I., VAŠEČKA, M. (2019). *Prevencia a boj proti radikalizácii v online prostredí*. Bratislava Policy Institute, Bratislava 2019. ISBN 978-80-973236-4-6. s.104

This paper was supported by the outputs of the feasibility study/analytical study “Motivational Elements in the Recruitment of Professional Soldiers of the Armed Forces of the Slovak Republic and Their Use by Recruitment Centers” NI4200645, funded by the Ministry of Defence of the Slovak Republic through the interdepartmental sub-programme 06E0I – Research and Development in Support of State Defence.

Mgr. Peter GAŽO
Akadémia ozbrojených síl generála M. R. Štefánika
Demänová 393, 031 01 Liptovský Mikuláš
E-mail: peter.gazo@aos.sk

PhDr., Mgr. Soňa ŠROBÁROVÁ, PhD., MBA, Ed.D.
Akadémia ozbrojených síl generála M. R. Štefánika
Demänová 393, 031 01 Liptovský Mikuláš
E-mail: sona.srobarova@aos.sk

doc. Ing. Lubomír BELAN, PhD.
Akadémia ozbrojených síl generála M. R. Štefánika
Demänová 393, 031 01 Liptovský Mikuláš
E-mail: lubomir.belan@aos.sk

PhDr. Mária MARTINSKÁ, PhD.
Akadémia ozbrojených síl generála M. R. Štefánika
Demänová 393, 031 01 Liptovský Mikuláš
E-mail: maria.martinska@aos.sk

DOI: https://doi.org/10.52651/vr.a.2025.3.88-105
VOJENSKÉ REFLEXIE
ISSN: 1336-9202 (online)
2025, Number 3, Page 88-105

ECONOMIC SECURITY IN THE FACE OF MIGRATION, CYBERATTACKS, AND POLITICAL CRISES

Łukasz BOJARSKI

ARTICLE HISTORY

Submitted: *28.10.2025*

Accepted: *27.11.2025*

Published: *31.12.2025*

ABSTRACT

In the scientific article, an attempt is made to conceptualize economic security under the overlapping conditions of illegal migration, cyberattacks, and political crises, which create interdependent vectors of risk within a fluid geopolitical order. The aim of the scientific article is to outline an analytical framework grounded in the Polish school of security studies—with reference to the work of Jan Maciejewski, Małgorzata Stochmal, Marian Cieślarczyk, Andrzej Pieczywok, and Janusz Gierszewski—and situated at the intersection of the sociology of politics and the sociology of crises. The analysis is based on theoretical and critical analysis of the subject literature, complemented by systems and comparative approaches characteristic of sociological security studies.

The mechanisms of the instrumentalization of migration within the logic of hybrid warfare and their effects on public finances, the labor market, and human capital are analyzed by the author of the scientific article. Particular attention is paid to the escalation of cyberattacks on critical infrastructure and financial systems, which reprofile the macroeconomic risk map and compel investment in cyber-resilience and business continuity management. The author also attempts to link political instability with disruptions to supply chains—especially in critical raw materials and rare earth minerals—which intensify the transmission of price and exchange-rate shocks.

In the financial dimension, it is shown that the effectiveness of open market operations and monetary policy transmission channels is constrained by heightened transaction and counterparty risks and by exchange-rate volatility; stress tests based on hybrid scenarios, supply-source diversification, and the development of digital competencies are advocated. In conclusion, it is indicated that the war in Ukraine and US–China tensions—with active roles played by India, the EU, and Russia—constitute a "new normal" of uncertainty, requiring the integration of migration, digital, and financial policies, as well as the continued promotion of Polish scholarly contributions

KEYWORDS

geopolitical order; economics; rare earth minerals; illegal migration; cyberattacks; human capital; sociology of politics; sociology of crises; sociology of risk.

INTRODUCTION: Economic Security as a Sociological Category

In the second and third decades of the twenty-first century, the notion of security has undergone profound redefinition. Its semantic field has expanded far beyond the military domain to include social, informational, and economic dimensions. Within this new configuration, economic security emerges as a strategic category that encapsulates the stability, resilience, and adaptive capacity of national economies exposed to complex transnational pressures. The overlapping crises of illegal migration, cyberattacks, and political instability have revealed the multidimensional character of economic security, transforming it from an abstract concept of state policy into a tangible determinant of everyday life.

In order to ground this analytical perspective more firmly, it is necessary to situate the concept of economic security within a broader theoretical framework. Such a framework is provided by the Polish school of security studies, which offers an interdisciplinary and sociologically informed understanding of security as a systemic and relational phenomenon.

Research Methods

The article employs research methods appropriate to theoretical studies in the fields of security studies and sociology. The primary research method is theoretical analysis combined with critical analysis of the subject literature, including the scholarly contributions of the Polish school of security studies (among others, Jan Maciejewski, Małgorzata Stochmal, Marian Cieślarczyk, Andrzej Pieczywok, and Janusz Gierszewski).

In addition, the method of systems analysis is applied in order to demonstrate the interdependencies between migration, cyberthreats, and political crises as components of a single system of economic risk. A comparative method is also employed, enabling the juxtaposition of different types of threats and their consequences for the economic stability of the state. Furthermore, an interpretative-sociological method is used to reconstruct the meanings of economic security under conditions of global uncertainty.

Theoretical Foundations of Economic Security Analysis in the Polish School of Security Studies

The Polish school of security studies has made a distinctive contribution to the conceptualisation of this phenomenon, emphasizing the interdisciplinary synthesis of sociology, economics, and political science. As Jan Maciejewski has argued, the modern understanding of security requires analytical categories that connect individual experience with systemic functionality, revealing how macro-level threats manifest as micro-level vulnerabilities. (Maciejewski, 2025, pp.45-26) In this view, economic security cannot be reduced to fiscal indicators or market performance; it must be understood as a dynamic process of safeguarding the material foundations of social order under conditions of uncertainty.

This sociological orientation is shared by Marian Cieślarczyk, who has long advocated an integrated approach linking economic, cultural, and moral dimensions of security. According to Cieślarczyk, security is "a holistic property of social systems, dependent on both their material resources and their axiological coherence" (Cieślarczyk, 2011, p. 73). In other words, the economic stability of a state depends not only on GDP or balance-of-trade figures but also on the integrity of its institutions, the trust of its citizens, and the quality of its human capital. The erosion of these intangible assets—through corruption, disinformation, or demographic decline - represents as grave a threat to economic security as inflation or recession.

The analytical framework developed by Małgorzata Stochmal adds yet another layer to this understanding. In her studies on security systems and crisis management, Stochmal emphasises that modern risk is systemic rather than episodic: it arises from the interdependence of technological, political, and social processes (Stochmal, 2020, pp.27-34). In this perspective, illegal migration, cyberattacks, and political crises are not isolated events but interconnected vectors of destabilisation. Each amplifies the others through feedback loops of mistrust, misinformation, and market reaction. Economic security, therefore, must be conceptualised not as the absence of risk but as the capacity to absorb and adapt to cascading shocks.

Andrzej Pieczywok, developing the Polish theory of security culture, situates economic security within the broader category of strategic security culture – a pattern of values, behaviours, and institutional practices that shape a society's response to threats (Pieczywok, 2015, pp.18-23). His work highlights that resilience is not solely technical or economic but also normative. A society that lacks a culture of responsibility, foresight, and solidarity is incapable of maintaining economic security even when equipped with advanced technologies or large financial reserves. The ability to manage crises thus becomes inseparable from the capacity to reproduce shared meaning and trust across economic institutions and political systems.

Janusz Gierszewski, in turn, has drawn attention to the operational dimension of security systems, stressing that their effectiveness depends on coherent management, transparent communication, and the coordination of public and private actors (Gierszewski, 2017, pp.66-79). His analytical model underscores that the economy and the security system form a mutually dependent structure: markets require stability and predictability to function, while state institutions depend on the economy's fiscal strength to sustain protective measures. This interdependence makes economic security both an end and an instrument – a self-referential field in which the safeguarding of value and the production of value coincide.

The sociological implication of these perspectives is that economic security cannot be separated from the social construction of risk. As Ulrich Beck and Anthony Giddens have observed, late modernity transforms risk from an external hazard into a constitutive element of governance and identity. In the Polish school, this insight takes on a pragmatic form:

security is not merely about defence but about adaptation - a process of continuous learning through crisis. Illegal migration, cyberattacks, and political instability are thus interpreted not only as threats to be neutralised but as tests of institutional flexibility and social cohesion.

From this theoretical standpoint, economic security appears as a multidimensional field structured by three principal logics: the logic of sovereignty, the logic of interdependence, and the logic of resilience. The logic of sovereignty refers to the state's capacity to regulate its borders, financial flows, and strategic resources. The logic of interdependence acknowledges the global nature of markets, technologies, and information systems that transcend national boundaries. The logic of resilience, finally, concerns the ability of societies to maintain functionality under stress - to anticipate, absorb, and recover from shocks without collapsing into chaos. The interplay of these three logics defines the architecture of contemporary security, where national autonomy and global integration coexist in permanent tension.

The present article proposes a sociological analysis of economic security under conditions of migratory, digital, and political turbulence. Its purpose is not to present a descriptive catalogue of risks, but to articulate a coherent interpretive framework in which the mechanisms of economic destabilisation can be understood as socially mediated processes. Illegal migration is examined as a phenomenon that not only strains labour markets and welfare systems but also serves as a tool of hybrid warfare, destabilising public trust and financial stability. Cyberattacks are analysed as a new form of economic violence - targeting the informational infrastructure that underpins transactions, banking systems, and trade. Political crises are discussed as catalysts of macroeconomic volatility, undermining investor confidence and fragmenting global supply chains, especially in the domain of rare earth minerals critical for advanced technologies.

The guiding assumption is that economic security cannot be achieved solely through technocratic regulation or military deterrence. It requires an integrative model of governance that links migration policy, cybersecurity, and financial stability under a unified strategic vision. The Polish tradition of security science, developed by Maciejewski and his colleagues, provides a conceptual foundation for such a model because it unites theoretical depth with pragmatic orientation. It insists that the economy is not an autonomous system but a domain of social relations—shaped by trust, authority, and cultural norms - and that threats to it are therefore inseparable from broader crises of legitimacy and solidarity.

This article will proceed by exploring, in turn, the three domains in which the fragility of economic security becomes most visible: illegal migration as a hybrid risk to labour and welfare systems; cyberattacks as a destabilising force in financial and industrial infrastructures; and political crises as accelerators of systemic uncertainty. Each section will show that these processes intersect in a common matrix of vulnerability, in which digital interdependence, geopolitical rivalry, and social fragmentation converge. The concluding section will situate these findings within the global "new normal" shaped by the war in Ukraine, the U.S. - China technological rivalry, and the strategic repositioning of India and the European Union.

In the logic of contemporary sociology of security, this inquiry is not simply diagnostic but reflective: it aims to clarify how societies conceptualise and manage uncertainty. The Polish school's insistence on human capital as the decisive factor of national security reminds us that the ultimate resource of any economy is its people - their competence, creativity, and moral responsibility. Economic security, in this sense, is not an end-state but a moral and cultural project, an ongoing negotiation between vulnerability and resilience, autonomy and interdependence, power and trust.

The theoretical perspectives outlined above provide a conceptual lens through which contemporary threats to economic security can be meaningfully interpreted. One of the most salient and multifaceted of these threats is irregular migration, which increasingly operates not only as a social or demographic phenomenon, but also as an instrument of hybrid pressure affecting economic stability.

Migration as a Hybrid Threat to Economic Security

The issue of migration has always accompanied the processes of globalisation, but in the twenty-first century it has assumed a new and distinctly strategic dimension. Illegal migration, far from being a purely humanitarian or demographic challenge, has become a factor of systemic destabilisation that penetrates the very structure of economic security. Within the European context, Poland finds itself at the intersection of two dynamics: on one hand, demographic decline and labour shortages necessitate controlled migration; on the other, the instrumentalisation of migratory flows by external actors transforms the phenomenon into a hybrid threat. In both cases, the state's economic resilience and fiscal balance become primary fields of tension.

The economic effects of large-scale irregular migration can be observed in three interrelated domains: the labour market, the welfare system, and public finance. The first of these, the labour market, reveals the ambivalence of migration: it mitigates workforce shortages in key sectors such as construction, logistics, and agriculture, while simultaneously producing pressure on wage structures and employment standards. Janusz Gierszewski notes that the influx of irregular labour "creates segmented employment systems, in which legality itself becomes a market variable" (Gierszewski, 2017, p. 93). In this sense, illegal migration generates an informal economy that coexists with formal structures, eroding the tax base and distorting competition.

From the perspective of economic security, such distortions have long-term consequences. They weaken the redistributive functions of the state, undermine trust in institutions, and increase the burden on public finances. Marian Cieślarczyk, analysing the ethical foundations of security systems, underlines that the erosion of fiscal integrity constitutes not only an economic risk but a moral one: “it corrodes the collective sense of justice that legitimises the fiscal system itself” (Cieślarczyk, 2011, p.75). When the social perception of fairness declines, so does willingness to contribute, creating a feedback loop of evasion and under-collection. The costs of integration, welfare assistance, and border protection then accumulate as structural deficits within state budgets.

Illegal migration also affects human capital - a category central to Polish security sociology. Małgorzata Stochmal emphasises that “a society’s resilience depends on the alignment of its human capital with its institutional capacities” (Stochmal, 2020, p. 46) . When migration is irregular, this alignment fails: educational systems, labour-market policy, and public administration cannot integrate new populations effectively. As a result, potential human resources are underutilised, while xenophobia and social fragmentation rise. The labour force may expand numerically but deteriorate qualitatively, as skills remain unrecognised and social capital erodes.

At the macroeconomic level, the financial consequences of uncontrolled migration manifest in higher fiscal expenditures on security, healthcare, and emergency accommodation. Recent analyses by the European Union Agency for Asylum (EUAA Report 2024) indicate that irregular migration increased the EU’s collective border-management spending by 32 percent between 2021 and 2023, while humanitarian outlays by national governments rose by 21 percent[1]. For Poland, positioned along the eastern frontier of the Schengen Area, these costs are multiplied by the geopolitical context: migration pressure is often orchestrated through proxy states as part of hybrid operations.

Hybrid warfare - the coordinated use of military, informational, and migratory tactics -transforms demographic movement into an instrument of economic coercion. Jan Maciejewski interprets such phenomena through the lens of dispositional groups, noting that “when state and non-state actors use populations as tools of pressure, the social order becomes the battlefield itself” (Maciejewski, 2025, pp. 88-91). The crisis at the Polish-Belarusian border in 2021 demonstrated this mechanism with stark clarity. Migrants were mobilised not as individuals seeking refuge but as vectors of disruption targeting logistics chains, energy infrastructure, and political stability. The ensuing fiscal expenditures on border fortification, emergency healthcare, and humanitarian management reached billions of złotych, diverting resources from development programmes and public investment.

The sociological dimension of this phenomenon lies in its cumulative effect on collective trust. As Cieślarczyk and Pieczywok jointly observed in their recent monograph Kultura bezpieczeństwa w warunkach niepewności globalnej (2023), “the use of migration as an element of pressure undermines citizens’ faith in the capacity of institutions to protect both

[1] European Union Agency for Asylum (EUAA), Annual Report 2024 on Asylum Trends, Brussels 2024, pp. 41–43

physical and economic security" (Cieślarczyk, Pieczywok, 2023, p. 119). When the public perceives the border as porous, it generalises that insecurity to the financial system and to the state as a whole. Market confidence, consumer optimism, and investment behaviour all deteriorate - illustrating how psychological insecurity translates directly into economic risk.

From the perspective of fiscal policy, migration-related expenditures create a dual burden: increased current spending and reduced long-term productivity. According to a 2024 report by the National Bank of Poland, the fiscal costs of border-security operations and refugee assistance amounted to 0.8 percent of GDP in 2022, while productivity growth in affected regions fell by 1.3 percent[2] . These data confirm that hybrid migration pressures are not temporary disturbances but structural shocks with measurable economic consequences.

Moreover, the financing of migration management increasingly relies on debt instruments and EU transfers, generating dependency that further constrains fiscal sovereignty. As Stochmal argues, "security financed through external credit transforms from protection into subordination" (Stochmal, op. cit., p. 57). This statement resonates strongly in the context of Poland's evolving position within the EU's financial architecture, where solidarity funds for border management coexist with macroeconomic conditionality. Economic security thus becomes a negotiation between autonomy and interdependence – a defining feature of the contemporary European order.

In sociological terms, illegal migration can be read as a stress test for the moral economy of security. The capacity to combine humanitarian obligations with fiscal prudence becomes the criterion of state maturity. When this balance collapses, two risks emerge: the securitisation of migration (which erodes democratic legitimacy) and the politicisation of economics (which replaces rational budgeting with populist spending). Andrzej Pieczywok warns that "a security culture devoid of axiological grounding degenerates into mere technocracy or propaganda" (Pieczywok, 2015, p. 28). The challenge, therefore, lies in constructing a normative framework that integrates human rights with economic rationality, avoiding both the cynicism of utilitarianism and the paralysis of moralism.

The complexity of the problem also stems from the interaction between migration and other hybrid threats. Disinformation campaigns exploit public fears, creating economic panic, capital flight, and speculative volatility. Social media amplify narratives of crisis, triggering behavioural responses that can destabilise markets. As noted by the Institute of Economic Forecasting (Warsaw 2025), "the perception of migration as chaos produces measurable economic losses through the mechanism of consumer pessimism"[3]. Hence, the management

[2] National Bank of Poland (NBP), Economic Security and Migration Pressures: Report 2024, Warsaw 2024, pp. 12–15

[3] Institute of Economic Forecasting (IEP), Perception of Migration and Economic Behaviour in Poland, Warsaw 2025, p. 6.

of migration is not only a logistical task but a communicative one: the economy depends as much on trust as on capital.

The intersection of migration and hybrid warfare thus redefines the parameters of economic security. It demands coordination among ministries of finance, interior, and defence; alignment between fiscal discipline and social inclusion; and strategic investment in border technology, labour-market regulation, and social integration. Above all, it requires a security culture — in the sense developed by Pieczywok and Cieślarczyk - that perceives the economy not as an isolated system but as a living organism whose vitality depends on ethical integrity and civic cohesion.

Illegal migration, when analysed through this lens, appears as both a threat and a mirror: it exposes the fragility of the economic system while revealing its moral foundations. The response to it will determine not only the stability of state budgets but the very legitimacy of governance in an era of interdependent crises.

While migration-related pressures expose the social and fiscal vulnerabilities of economic systems, they do not exhaust the spectrum of hybrid threats shaping contemporary insecurity. An equally destabilising factor emerges in the digital domain, where cyberattacks target the informational infrastructure upon which modern economies depend.

Cyberattacks and Cyberthreats as Factors of Economic Destabilisation

If the economy of the twentieth century depended on the flow of goods, the economy of the twenty-first depends on the flow of information. Financial systems, energy grids, transport logistics, and supply chains are all mediated by digital technologies. Consequently, the primary vulnerability of contemporary economies no longer lies in their material production but in their informational architecture. A single cyberattack can paralyse entire markets, distort exchange rates, or destroy the credibility of public institutions. As Małgorzata Stochmal notes, "information has become the critical infrastructure of security, and its disturbance is equivalent to the disruption of the state itself" (Stochmal, 2020, p. 58).

The growing frequency and sophistication of cyberattacks have revealed that economic security must now be conceptualised as cyber-economic security: a composite of financial resilience, digital protection, and institutional trust. Poland, like other European countries, has experienced a steady escalation of cyber incidents targeting banking systems, government platforms, and strategic industries. According to the 2024 National Cybersecurity Report of the Ministry of Digital Affairs, the number of financially motivated cyberattacks increased by 37 percent in 2023 compared to the previous year.[4] These attacks include ransomware assaults on small and medium enterprises, phishing campaigns targeting online banking users, and data breaches affecting public institutions.

[4] Ministry of Digital Affairs, National Cybersecurity Report 2024, Warsaw 2024, pp. 9–11.

The economic implications of such incidents are both direct and systemic. Direct losses include ransom payments, data restoration costs, and service interruptions. Systemic losses, however, manifest as erosion of trust in financial institutions and payment systems - what sociologists of security term symbolic destabilisation. Janusz Gierszewski emphasises that "the financial market functions as a trust system; its collapse does not begin with bankruptcy but with disbelief" (Gierszewski, 2017, p. 122). Once trust erodes, liquidity and investment decline, triggering fiscal instability and social anxiety.

Cyberattacks on financial systems often function as strategic tools of hybrid warfare. They blur the boundary between economic competition and political hostility. In 2022–2023, Polish financial institutions were repeatedly targeted by cyber operations traced to state-sponsored groups linked to Russia and Belarus. The purpose of these attacks was not simply monetary gain but psychological destabilisation - to undermine confidence in the state's ability to safeguard digital sovereignty. In this context, economic security and cybersecurity converge: the digital battlefield becomes an arena where fiscal stability and national credibility are contested simultaneously.

From a sociological perspective, cyberattacks operate as mechanisms of symbolic violence in the Bourdieusian sense: they manipulate the cognitive and emotional environment of societies rather than their material base. They exploit the modern individual's dependence on digital tools - banking apps, e-commerce, social networks - to generate a pervasive sense of vulnerability. As Cieślarczyk argues, "the loss of informational security induces not only financial anxiety but existential uncertainty, undermining the moral order on which economic cooperation rests" (Cieślarczyk, 2011, p. 104).

In response, the Polish school of security studies emphasises the cultivation of security culture as a prerequisite for digital resilience. Andrzej Pieczywok defines security culture as "a set of values and practices that condition the rational use of technology and the responsible management of risk" (Pieczywok, 2015, p. 39). This concept underscores that cybersecurity cannot rely solely on technical defence systems; it requires human and organisational maturity. Training programmes, ethical standards, and institutional transparency form the social infrastructure of cyber-resilience.

In the economic sphere, this translates into the creation of adaptive systems that can anticipate, absorb, and recover from digital shocks. The European Central Bank's 2024 Cyber Resilience Report emphasises that financial institutions must develop "redundancy and continuity protocols that treat cyberattacks as inevitable, not exceptional".[5] Polish banks, particularly those integrated into European payment systems, have begun implementing such frameworks, guided by the EU's Digital Operational Resilience Act (DORA), which entered into force in 2025. Yet compliance remains uneven, especially among smaller institutions lacking financial or human resources.

[5] European Central Bank, Cyber Resilience Report, Frankfurt 2024, pp. 17–20.

The sociological challenge lies in integrating these technical standards with public consciousness. As Stochmal points out, "technological resilience without social awareness is like a wall without a foundation". (Stochmal, op. cit., p. 64) Public education in cybersecurity - from schools to workplaces - is therefore an essential component of economic security. The Ministry of Education's 2025 Cyber Literacy Strategy seeks to embed such education across curricula, reflecting an awareness that digital competence is now as fundamental as literacy itself.

Cyberattacks also expose the geopolitical dimension of economic vulnerability. In the post-pandemic period, global supply chains have become targets of digital espionage and sabotage. Attacks on semiconductor producers, energy distributors, and logistics software providers demonstrate that control over information equates to control over resources. Maciejewski's theory of dispositional groups helps interpret this dynamic: in cyberspace, traditional military hierarchies dissolve into flexible, transnational networks capable of rapid offensive or defensive adaptation. (Maciejewski, 2025, pp. 111-114) These networks – whether state-based or criminal – function as "digital armies," operating in the grey zone between legality and warfare.

In Poland, the 2023 ransomware attack on the Poczta Polska logistics system disrupted financial transactions and delivery chains for several days, causing measurable economic losses estimated at 0.04 percent of GDP.[6] The incident demonstrated that even peripheral institutions within the economic system can become points of strategic vulnerability. Sociologically, such cases reveal the interdependence of micro and macro processes: the failure of one node triggers cascading effects across entire networks of trust, supply, and payment.

The human dimension of cyberattacks is equally important. Research by the Institute for Security Culture and Digital Ethics (Warsaw, 2024) shows that employees remain the weakest link in digital protection. Over 60 percent of successful cyber intrusions in Poland originate from social engineering – manipulation rather than hacking[7] . This confirms that economic security depends not merely on encryption or firewalls but on the ethical discipline and situational awareness of individuals. The digital battlefield, in this sense, is primarily sociological: a struggle for attention, perception, and moral vigilance.

In the financial sector, central banks face a paradox: the more they digitalise, the more vulnerable they become. The introduction of digital currencies and algorithmic trading increases efficiency but simultaneously creates systemic fragility. The Polish National Bank's 2025 analysis warns that "algorithmic interdependencies can amplify minor cyber incidents into macroeconomic disturbances". [8] The interconnectivity of trading systems, clearing

[6] Polish Economic Institute, Cyber Incident Economic Impact Study 2023, Warsaw 2024, p. 7.

[7] Institute for Security Culture and Digital Ethics, Human Factors in Cybersecurity, Warsaw 2024, p. 15.

[8] National Bank of Poland, Algorithmic Finance and Cyber Risk, Warsaw 2025, p. 23.

houses, and fintech platforms thus turns economic modernisation into a double-edged sword - enhancing competitiveness while multiplying risks.

The theoretical synthesis offered by Cieślarczyk and Gierszewski suggests that economic security in the digital age must integrate three levels: technological infrastructure, organisational adaptability, and cultural trust. Each failure - technical, bureaucratic, or moral — opens a gate for destabilisation. Therefore, policies focused exclusively on cybersecurity technology without attention to institutional ethics or public education risk creating what Stochmal calls "a defensive illusion" (Stochmal, op. cit., p. 72). The economy remains exposed not because of insufficient tools but because of insufficient culture.

Finally, the sociological implications of cyberthreats extend beyond economics. They shape the emotional climate of societies, reinforcing feelings of precariousness and control loss. These affective states, in turn, influence consumption, savings, and investment behaviour. As Pieczywok warns, "the economy of fear precedes the economy of loss" (Pieczywok, 2015, p. 45). Hence, cultivating resilience means not only defending networks but restoring confidence – a psychological and moral project as much as a technical one.

Cyberattacks reveal the deep interdependence of security, economy, and social consciousness. They expose the paradox of digital modernity: that progress itself produces new vulnerabilities. In this sense, cyber-resilience becomes a metaphor for the entire security system — a constant process of learning, adaptation, and moral reconstruction within a fragile global order.

Although cyberthreats primarily operate within the digital and financial infrastructure of the economy, their effects are deeply entangled with broader political dynamics. In this sense, cyber insecurity intersects with political crises, which amplify economic volatility and transform uncertainty into a systemic condition of governance.

Political Crises and Financial and Monetary Stability

Political crises have always had economic consequences, yet in the globalised and digitalised world of the twenty-first century they have become triggers of systemic financial turbulence. The modern economy operates under conditions of interdependence so dense that the volatility of one political centre can generate reverberations across continents. In such circumstances, economic security must be analysed not merely as the stability of national markets but as the capacity to manage interlinked crises that are simultaneously fiscal, monetary, and political.

In the Polish school of security studies, Jan Maciejewski defines dispositional systems as institutional structures that "must maintain equilibrium under conditions of uncertainty by transforming potential chaos into controlled adaptation" (Maciejewski, 2025, p. 143). This definition applies with particular force to the relationship between political decision-making and financial governance. Monetary institutions such as central banks act as dispositional groups of the economy: their task is to preserve trust in the value of money despite political oscillations. Yet, as recent years have shown, that trust is fragile.

Between 2020 and 2024, the world economy faced a concatenation of crises - pandemic disruption, Russia's aggression against Ukraine, energy price shocks, and growing rivalry between the United States and China. Each episode revealed the sensitivity of open market operations (OMOs) – the key instrument of central banks for controlling liquidity – to geopolitical uncertainty. When political risk rises, OMOs cease to be a purely technical tool and become instruments of strategic communication. Their effectiveness depends less on quantitative ratios than on the credibility of policy and the cohesion of institutions. As Janusz Gierszewski observes, "economic security is first a matter of confidence, and confidence is a political product" (Gierszewski, 2017, p. 156).

The war in Ukraine provides a paradigmatic example. The Polish National Bank (NBP) faced unprecedented pressure to stabilise the złoty, control inflation, and simultaneously finance state expenditure on defence and humanitarian support. Each decision regarding bond purchases or interest-rate adjustments was interpreted by markets through the prism of political risk. According to the NBP's 2024 Report on Monetary Stability, fluctuations in sovereign-bond yields were three times more sensitive to geopolitical events than to macroeconomic indicators.[9] The implication is clear: in times of political crisis, monetary instruments become channels through which insecurity is transmitted rather than neutralised.

From a sociological standpoint, this dynamic exemplifies what Małgorzata Stochmal calls "the reflexivity of risk in security systems" (Stochmal, 2020, p. 81). Political crises do not simply affect economies externally; they are internalised as expectations, anxieties, and anticipatory behaviours within markets. Investors act on perceptions of instability, thereby materialising the very risks they fear. The self-fulfilling nature of financial panic transforms subjective uncertainty into objective volatility. Thus, the sociology of security must complement economic analysis: it explains why rational policies may fail when collective trust disintegrates.

The interconnection between political credibility and monetary stability is particularly visible in the domain of open market operations. These consist of central-bank purchases and sales of government securities designed to regulate money supply. In stable conditions, OMOs provide liquidity and signal confidence. Under political duress, however, they risk being perceived as emergency measures, eroding rather than restoring faith. The European Central Bank's 2023 review of post-pandemic operations notes that "repeated interventions under uncertain political governance produce diminishing marginal trust effects".[10] In other words, when political conflict dominates fiscal policy, even correct monetary instruments lose symbolic power.

[9] National Bank of Poland (NBP), Report on Monetary Stability 2024, Warsaw 2024, pp. 5–8.

[10] European Central Bank, Post-Pandemic OMOs Review, Frankfurt 2023, p. 19.

For Poland, a country structurally embedded in the European Union's financial ecosystem yet exposed to eastern geopolitical turbulence, the coordination of monetary and political strategies has become a key determinant of economic security. Marian Cieślarczyk underlines that "systemic resilience depends on the moral and cognitive integration of decision-makers; a state cannot protect its currency if its elites are divided by short-term interests". (Cieślarczyk, 2011, p. 119) The institutional fragmentation observable in many democracies - oscillating coalitions, populist cycles, politicisation of central banks - directly threatens macroeconomic coherence.

Global financial flows amplify these vulnerabilities. The instantaneous mobility of capital allows investors to react to political signals within seconds. As the IMF's World Economic Outlook 2024 reports, political-risk variables accounted for nearly 40 percent of cross-border capital-flow volatility in emerging Europe[11]. Economic security, therefore, becomes hostage to the narrative discipline of governments. A single tweet by a political leader, a corruption scandal, or a sudden change of coalition can trigger speculative movements that outweigh the effects of months of prudent economic management.

This fragility has structural causes. The financialisation of the global economy has created a situation in which symbolic indicators – credit ratings, forecasts, political statements — exert greater influence than material production. As Pieczywok warns, "when meaning governs money, the ethical deficit of politics becomes an economic hazard". (Pieczywok, 2015, p. 51). Political crises thus threaten not only fiscal balances but the moral architecture of capitalism itself.

At the operational level, central banks have attempted to counteract these pressures through expanded OMOs and quantitative-easing measures. Yet, as the Bank for International Settlements (BIS Report 2023) observes, such policies entail a paradox: "the more liquidity central banks inject to offset political risk, the more markets become dependent on political stability"[12] . The economy enters a cycle of addiction to reassurance, in which every new crisis demands stronger intervention. This mechanism transforms the state into both guarantor and prisoner of financial expectations.

The sociological dimension of this process is crucial. Trust, once eroded, cannot be restored by decree; it must be rebuilt through consistent communication and symbolic credibility. Stochmal and Gierszewski in their 2024 paper Economic Governance and Social Resilience argue that "economic security is co-produced by narratives of stability - monetary policy is therefore a form of social pedagogy". (Stochmal, Gierszewski, 2024, p. 14) The state must teach society how to interpret uncertainty, transforming panic into patience.

[11] International Monetary Fund (IMF), World Economic Outlook 2024, Washington 2024, p. 67.

[12] Bank for International Settlements (BIS), Annual Economic Report 2023, Basel 2023, p. 32.

In the Polish context, political polarisation remains a latent threat to such pedagogical coherence. Changes in fiscal priorities accompanying electoral cycles often undermine long-term investment policy. The 2024 Polish Economic Forum report notes that private investment growth in Poland was 2.1 percent lower in election years than in non-election years[13]. This correlation underscores the cost of political volatility: it depresses innovation, weakens capital formation, and slows adaptation to technological change – all fundamental pillars of economic security.

Globally, the rivalry between the United States and China, the growing role of India, and the strategic repositioning of the European Union have intensified this interdependence. The weaponisation of trade, the politicisation of rare-earth-mineral supply chains, and the emergence of "economic blocs of trust" indicate that political crises are no longer episodic but structural features of the international order. The OECD's Security and Markets Report 2025 predicts that by 2030, 20 percent of global trade will occur within politically aligned blocs rather than through open markets[14]. Such fragmentation challenges the liberal vision of a self-regulating global economy and demands a new sociological understanding of interdependence.

Within this reconfigured landscape, economic security requires both diversification and resilience. Poland's growing engagement with EU energy policy, transatlantic defence cooperation, and Asian investment flows illustrates how middle powers navigate between dependence and autonomy. As Cieślarczyk reminds, "the real measure of sovereignty is not isolation but the capacity to cooperate without subordination". (Cieślarczyk, 2011, p. 125)

Ultimately, political crises function as stress tests for the moral and institutional cohesion of societies. Their economic effects are not limited to GDP fluctuations; they reveal the depth of social trust, the maturity of governance, and the quality of leadership. The sociology of security, building on the works of Maciejewski and his successors, teaches that crises can also be opportunities for renewal – moments when collective reflection replaces routine. Economic security in such conditions becomes not a shield but a process of continuous self-correction, sustained by transparency, solidarity, and disciplined optimism.

The economic consequences of political crises cannot be fully understood in isolation from the wider transformations of the international system. These crises unfold within an emerging global order characterised by strategic rivalry, fragmented supply chains, and the growing politicisation of economic interdependence.

[13] Polish Economic Forum, Investment and Political Cycles Report 2024, Warsaw 2024, p. 9.

[14] OECD, Security and Markets Report 2025, Paris 2025, p. 23.

The New Global Order and Its Implications for Economic Security

The multifaceted processes examined above - irregular migration, cyberattacks, and political crises - converge within a single analytical horizon: the reconfiguration of global economic security in the early twenty-first century. In this horizon, security is no longer a peripheral condition of prosperity but its very foundation. Without institutional credibility, technological resilience, and social trust, economic systems fragment under the pressure of global turbulence. The Polish school of security studies – from Maciejewski's theory of dispositional groups to Stochmal's systemic-risk analysis and Cieślarczyk's axiological concept of resilience – provides a conceptual architecture capable of explaining this transformation.

The war in Ukraine, more than any recent event, has exposed the interdependence of military, political, and economic domains. Beyond the humanitarian catastrophe and geopolitical upheaval, the conflict has produced deep structural shifts in energy markets, food supply chains, and fiscal policies across Europe. Poland's role as a logistical and humanitarian hub has revealed both the strength and fragility of its economic-security system. On one hand, defence-related spending and international aid have stimulated industrial production; on the other, the reallocation of resources and rising inflation have constrained fiscal flexibility. According to the NBP Economic Outlook 2025, the cumulative cost of war-related expenditures between 2022 and 2024 reached nearly 3 percent of Poland's GDP[15].

Yet, as Janusz Gierszewski reminds, "security costs are not losses when they strengthen systemic adaptability". (Gierszewski, 2017, p. 168) The investment in border infrastructure, energy diversification, and digital protection has accelerated Poland's strategic autonomy. Nevertheless, these advances remain conditioned by broader geopolitical tensions, particularly those between the United States and China. The emerging bipolarity of the global economy – centred on technological ecosystems and rare-earth mineral supply chains – has forced medium-sized states to navigate complex dependencies.

China's growing dominance in rare-earth markets, essential for electronics, defence, and renewable-energy technologies, poses a long-term challenge to economic sovereignty. The OECD Strategic Minerals Report 2024 notes that the PRC controls nearly 60 percent of global rare-earth processing capacity [16] . This concentration transforms materials into instruments of political leverage. As Cieślarczyk observes, "control over resources today functions as control over possibilities". (Cieślarczyk, 2011, p. 132) The ability to access, refine, and recycle these minerals will determine the technological and security position of states throughout the coming decade.

The United States, responding through the CHIPS and Science Act and strategic partnerships with allies, seeks to maintain technological primacy. Poland's participation in the

[15] National Bank of Poland, Economic Outlook 2025, Warsaw 2025, p. 7.

[16] Strategic Minerals Report 2024, Paris 2024, p. 11.

EU's Critical Raw Materials Alliance (2024) situates it within a European effort to balance these asymmetries. However, as Małgorzata Stochmal warns, "autonomy pursued through fragmentation risks creating islands of security amid oceans of dependency". (Stochmal, 2020, p. 93) The European Union must therefore integrate industrial policy with social cohesion - ensuring that economic resilience does not degenerate into protectionism.

India's ascent adds another layer of complexity. As a demographic and technological power, it occupies an intermediate position between the Western and Chinese blocs. Its expanding cooperation with the EU and Poland in sectors such as IT and pharmaceuticals signals the formation of a multipolar economic-security architecture. This diversification mitigates risk but also multiplies strategic calculations: interdependence now demands continuous negotiation rather than stable alignment.

From a sociological perspective, these global shifts redefine the meaning of economic resilience. It is no longer sufficient to maintain fiscal stability; states must cultivate adaptive intelligence — the collective capacity to reinterpret crises as opportunities. Cieślarczyk and Pieczywok, in their 2023 study Kultura bezpieczeństwa w warunkach niepewności globalnej, describe resilience as "the moral and cognitive ability to transform uncertainty into learning". (Cieślarczyk, A. Pieczywok, 2023, p. 142) Economic security thus depends not solely on the abundance of resources but on the quality of collective reasoning.

This insight has direct implications for Poland and other medium-sized economies. In an environment of accelerating digitalisation, demographic change, and ecological pressure, security must be reimagined as a multilevel ecosystem. Migration, cyberthreats, and political volatility are not discrete variables but interacting feedback loops. Their convergence requires what Stochmal calls "integrated strategic governance" – a coordination of economic, informational, and social subsystems under a shared normative vision. (Stochmal, op. cit., p. 101)

The normative dimension is essential. As Andrzej Pieczywok emphasises, "without axiological integration, the security system becomes efficient yet blind". (Pieczywok, 2015. P. 53) The defence of markets, currencies, and technologies must be guided by ethical coherence - respect for human dignity, legal order, and intergenerational responsibility. In the absence of such grounding, even the most sophisticated systems succumb to cynicism and opportunism, which ultimately erode the trust on which economies rest.

From this vantage point, the sociology of security reveals its full analytical potential. It shows that the economy is not an autonomous machine but a social contract maintained by confidence and recognition. Illegal migration, cybercrime, and political conflict each threaten this contract in distinct ways: by disrupting labour markets, corrupting informational networks, or discrediting governance. Yet, they also expose the pathways to renewal. Each crisis can strengthen institutional reflexivity and moral solidarity - if interpreted not as disaster but as feedback.

Looking forward, three challenges will determine the trajectory of economic security. First, the management of energy and mineral dependencies, requiring new partnerships and technological innovation. Second, the establishment of digital sovereignty - ensuring control over data, infrastructure, and algorithms. Third, the reconstruction of social capital eroded by populism, inequality, and disinformation. These tasks are interdependent: no algorithm can secure a society that distrusts its institutions, and no policy can succeed without public participation.

The war in Ukraine will remain the defining context for Europe's security culture. It has reminded societies that prosperity without preparedness is an illusion. Yet, it has also demonstrated that resilience is cumulative: every reform in education, energy, and governance strengthens deterrence. As Gierszewski concludes, "the front line of modern security runs through the economy, but its foundation lies in ethics". (Gierszewski, op. cit., p. 172)

The interactions between migration pressures, cyberthreats, and political instability thus converge into a coherent pattern of systemic risk. This convergence calls for a synthetic assessment of economic security, one that moves beyond sectoral analysis toward an integrated sociological interpretation.

CONCLUSION

In sum, *economic security in the face of migration, cyberattacks, and political crises* is not a technocratic agenda but a civilisational choice. It demands the integration of financial rationality with moral responsibility, global cooperation with national sovereignty, and technological innovation with human solidarity. The Polish contribution to security science, deeply rooted in sociological reflection and axiological realism, offers precisely this synthesis. It reminds us that the economy, like the state itself, survives not through fear of loss but through the discipline of trust.

REFERENCES

Bank for International Settlements (BIS), Annual Economic Report 2023, Basel 2023.

CIEŚLARCZYK, M. 2011. *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i obronności państwa*, Siedlce 2011. Wydawnictwo Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. ISBN: 9788370516147, s. 249

CIEŚLARCZYK M., PIECZYWOK A. 2023. *Kultura bezpieczeństwa w warunkach niepewności globalnej*, Warszawa 2023. s

European Central Bank, Post-Pandemic OMOs Review, Frankfurt 2023.

European Union Agency for Asylum (EUAA), Annual Report 2024 on Asylum Trends, Brussels 2024.

GIERSZEWSKI, J. 2017. *System bezpieczeństwa państwa. Ujęcie teoretyczne i praktyczne*, Gdańsk 2017.

Institute for Security Culture and Digital Ethics, Human Factors in Cybersecurity, Warsaw 2024.

International Monetary Fund (IMF), World Economic Outlook 2024, Washington 2024.

MACIEJEWSKI, J. 2025. *Grupy dyspozycyjne. Analiza socjologiczna*, 3rd ed., Wydawnictwo Uniwersytetu Wrocławskiego. Wrocław 2025. ISBN 978-83-229-4040-2. 26.s.

National Bank of Poland (NBP), Economic Outlook 2025; Report on Monetary Stability 2024; Algorithmic Finance and Cyber Risk, Warsaw 2024–2025.

PIECZYWOK, A. 2015*. Kultura bezpieczeństwa narodowego*. Ujęcie systemowe, Warszawa 2015. https://doi.org/10.15804/ppk.2015.02.06

STOCHMAL, M. 2020. *Zarządzanie bezpieczeństwem w warunkach ryzyka systemowego*, Lublin 2020.

STOCHMAL, M., GIERSZEWSKI J. 2024. "*Economic Governance and Social Resilience*," Security & Society Review, vol. 5(2), 2024.

OECD, Security and Markets Report 2025; Strategic Minerals Report 2024, Paris 2024–2025.

Polish Economic Forum, Investment and Political Cycles Report 2024, Warsaw 2024.

Polish Economic Institute, Cyber Incident Economic Impact Study 2023, Warsaw 2024.

mgr Łukasz Bojarski
ORCID 0009-0002-9621-4603
PhD student
Institute of International and Security Studies
Faculty of Social Sciences
University of Wrocław

Information for authors:

Submission deadline

- for papers to be published in **issue 1** in Slovak / Czech language **30th April**
- for papers to be published in **issue 2** in Slovak / Czech language **30th October**
- for papers to be published in **issue 3** in English language **30th October**

Template **- http://vr.aos.sk/index.php/en/for-authors-vr.html**

VOJENSKÉ REFLEXIE

AOS

VOJENSKÉ REFLEXIE

Military science journal

Publisher:

Akadémia ozbrojených síl
generála Milana Rastislava Štefánika
Demänová 393
031 01 Liptovský Mikuláš

Electronical journal published on internet with free access
http://vr.aos.sk/index.php/sk/

Published twice a year in Slovak/Czech and once a year in English

Number of pages: 106

Published:

December 2025, Volume XIX, Issue 3/2025
Photocover: Peter POLDRUHÁK
Cover: Dušan SALAK

ISSN 1336-9202 DOI https://doi.org/10.52651/vr.j.2025.3

AKADÉMIA OZBROJENÝCH SÍL
GENERÁLA MILANA RASTISLAVA ŠTEFÁNIKA