A U S P I C I A

Recenzovaný vědecký časopis pro oblast společenských a humanitních věd

Reviewed Scholarly Journal Dealing with Social Sciences

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ
ČESKÉ BUDĚJOVICE
VYSOKÁ ŠKOLA TECHNICKÁ A EKONOMICKÁ – ÚSTAV PODNIKOVÉ STRATEGIE
ČESKÉ BUDĚJOVICE
Ročník XXII, číslo 2

2025

AUSPICIA
Recenzovaný vědecký časopis pro otázky společenských a humanitních věd.
Založen v roce 2004. Vydáván Vysokou školou evropských a regionálních studií, České Budějovice, Česká republika a Vysokou školou technickou a ekonomickou, České Budějovice, Česká republika.

Rada pro výzkum, vývoj a inovace jako odborný a poradní orgán vlády ČR zařadila recenzovaný vědecký časopis Auspicia pro rok 2015 mezi recenzované neimpaktované časopisy, které uvedla v oborech Národního referenčního rámce excelence (NRRE).

V roce 2016 byl recenzovaný vědecký časopis Auspicia zařazen do mezinárodní databáze ERIH PLUS a od roku 2024 do online knihovny pro střední a východní Evropu – CEEOL.

AUSPICIA
A peer-reviewed scholarly journal for questions of the social sciences and humanities.
Founded in 2004. Published by The College of European and Regional Studies, České Budějovice, Czech Republic and The Institute of Technology and Business, České Budějovice, Czech Republic.

The Research, Development and Innovation Council, as a professional and consultative body of the Government of the Czech Republic, indexed Auspicia – a peer-reviewed scholarly journal on a list of peer-reviewed non-impacted journals in 2015, being published in the fields of the National Reference Framework of Excellence.

In 2016 Auspicia – a peer-reviewed scholarly journal was indexed in the international database ERIH PLUS and since 2024, it has been indexed in the Central and Eastern Europe Online Library – CEEOL.

Adresa redakce: Vysoká škola evropských a regionálních studií, z. ú., Žižkova tř. 1632/5b, 370 01 České Budějovice, tel.: 00420 386 116 839, https://auspicia.cz. Vychází dvakrát ročně v elektronické verzi (od roku 2019). **Prosinec 2025**. Časopis je financován VŠERS a VŠTE. **ISSN 2464-7217 (Online)**. **DOI: 10.36682/a_2025_2**.

Editorial Office Address: Vysoká škola evropských a regionálních studií, z. ú., Žižkova tř. 1632/5b, 370 01 České Budějovice, tel.: 00420 386 116 839, https://auspicia.cz. It has been published twice a year electronically (since 2019). **December 2025**. This journal is financed by The College of European and Regional Studies and The Institute of Technology and Business. **ISSN 2464-7217 (Online)**. **DOI: 10.36682/a_2025_2.**

EDIČNÍ RADA VŠERS · EDITORIAL BOARD OF VŠERS

Předseda ediční rady · Chairman of the Editorial Board
doc. Ing. Jiří **DUŠEK**, Ph.D.

Interní členové · Internal Members
doc. JUDr. PhDr. Jiří **BÍLÝ**, CSc.; PhDr. Jan **ČÁP**, Ph.D.; RNDr. Růžena **FEREBAUEROVÁ**; PhDr. Jan **GREGOR**, Ph.D.; doc. Ing. Marie **HESKOVÁ**, CSc.; PhDr. Štěpán **KAVAN**, Ph.D.; Mgr. Josef **KŘÍHA**, PhD.; doc. PhDr. Miroslav **SAPÍK**, Ph.D.; doc. Ing. Ladislav **SKOŘEPA**, Ph.D.; doc. Ing. Jaroslav **SLEPECKÝ**, PhD, MBA.; doc. JUDr. Roman **SVATOŠ**, Ph.D.

Externí členové · External Members
Ing. Jiří **ALINA**, Ph.D. *(Jihočeská univerzita, České Budějovice,* **ČR***)*; doc. PhDr. PaedDr. Silvia **BARNOVÁ**, PhD., MBA (Vysoká škola *DTI*, **Slovensko**); prof. Berislav **BOLFEK**, Ph.D. (*Zadarská univerzita, Zadar*, **Chorvatsko**); doc. dr. sc. Jurica **BOSNA** (*Zadarská univerzita, Zadar*, **Chorvatsko)**; doc. Ing. Jozefína **DROTÁROVÁ**, PhD., MBA (*Vysoká škola bezpečnostného manažérstva v Košiciach*, **Slovensko**); doc. MUDr. Lenka **HODAČOVÁ**, Ph.D. *(Univerzita Karlova, Hradec Králové,* **ČR***)*; doc. Ing. Petra **PÁRTLOVÁ**, Ph.D. (*Vysoká škola technická a ekonomická v Českých Budějovicích*, **ČR**); prof. PhDr. Miroslava **SZARKOVÁ**, CSc. *(Ekonomická univerzita, Bratislava,* **Slovensko***)*; doc. Ing. Jarmila **STRAKOVÁ**, Ph.D. *(Vysoká škola technická a ekonomická v Českých Budějovicích,* **ČR***)*

REDAKCE ČASOPISU AUSPICIA · EDITORIAL OFFICE OF JOURNAL AUSPICIA

Předseda redakční rady · Chairman of the Editorial Board
doc. Ing. Jiří **DUŠEK**, Ph.D. *(Vysoká škola evropských a regionálních studií, České Budějovice,* ***ČR****)*

Místopředseda redakční rady · Vice-chairman of the Editorial Board
doc. et doc. PaedDr. Mgr. Zdeněk **CAHA**, Ph.D., MBA, MSc. *(Vysoká škola technická a ekonomická v Českých Budějovicích,* ***ČR****)*

Šéfredaktor · Editor-in-Chief
doc. PhDr. Miroslav **SAPÍK**, Ph.D.

Výkonný redaktor · Managing Editor
doc. PhDr. Miroslav **SAPÍK**, Ph.D.

Technická redaktorka · Technical Editor
RNDr. Růžena **FEREBAUEROVÁ**

Redaktoři anglických textů · English Language Editors
Centrum jazykových služeb Vysoké školy technické a ekonomické

ČLENOVÉ MEZINÁRODNÍ REDAKČNÍ RADY (26) · MEMBERS OF THE INTERNATIONAL EDITORIAL BOARD (26)

OBSAH

BEZPEČNOST

VEŘEJNÁ SPRÁVA, MANAGEMENT

CONTENTS

BEZPEČNOST • SAFETY

DOI: 10.36682/a_2025_2_1

THREATS AND OPPORTUNITIES OF USING ARTIFICIAL INTELLIGENCE FROM A CYBERSECURITY PERSPECTIVE

Hrozby a príležitosti využívania umelej inteligencie z hľadiska kybernetickej bezpečnosti

Jana ZACHAR KUCHTOVÁ

Bratislava, Slovak Republic

ABSTRACT: The article analyses the potential threats and opportunities associated with the use of artificial intelligence in cybersecurity. The aim is to identify the key risks arising from the proliferation of advanced technologies, especially concerning their misuse in cyberattacks, hybrid operations, and autonomous decision-making processes. At the same time, it examines the positive potential of artificial intelligence in threat detection, big data analysis, and the strengthening of active defence in cyberspace. The article employs a combination of analytical and comparative approaches, drawing upon current scientific studies, technical reports, and strategic documents. The findings indicate the need for a balanced approach that considers technological, ethical, legislative, and geopolitical dimensions. The article contributes to the ongoing discussion on the responsible integration of artificial intelligence into cybersecurity policies and practices.

Key words: Artificial intelligence – cyber security – threats – opportunities – challenges

ABSTRAKT: Článok sa zaoberá analýzou potenciálnych hrozieb a príležitostí využívania umelej inteligencie v oblasti kybernetickej bezpečnosti. Cieľom je identifikovať hlavné riziká spojené s rozmachom pokročilých technológií, najmä z hľadiska ich zneužitia v rámci kybernetických útokov, hybridných operácií a autonómnych rozhodovacích procesov. Zároveň skúma pozitívny potenciál umelej inteligencie pri detekcii hrozieb, analýze veľkých dát a posilňovaní aktívnej obrany v kyberpriestore. V článku sa uplatňuje kombinácia analytického a komparatívneho prístupu, pričom autorka čerpá zo súčasných vedeckých štúdií, technických správ a strategických dokumentov. Výsledky naznačujú potrebu vyváženého prístupu, ktorý zohľadňuje technologické, etické, legislatívne aj geopolitické dimenzie. Práca prispieva k prebiehajúcej diskusii o tom, ako možno umelú inteligenciu zodpovedne integrovať do politík a praxe kybernetickej bezpečnosti.

Kľúčové slová: Umelá inteligencia – kybernetická bezpečnosť – hrozby – príležitosti – výzvy

INTRODUCTION

The development of human civilization in the 21st century is highly dynamic, volatile, unstable, and in many cases, markedly turbulent, bringing about profound changes across all areas, spheres, and sectors of society (Ivančík, 2021). Among the sectors experiencing the most dynamic transformation are security and technology. In the field of security, these changes are particularly evident in the evolving global and regional security environment, fundamental shifts in security conditions at both proximate and distant levels, and the emergence of new, asymmetrical security threats (Ivančík, Kazanský, 2023). In the sphere of technology, this development is most significantly reflected in advances in communication and information systems and tools, social media, nano-, bio-, and cloud technologies, quantum computing, automation, digitalization, robotics, the Internet of Things, and related fields.

In recent years, there has also been an unprecedented advancement in artificial intelligence (AI), which, among many other domains, – significantly impacts the dynamics of the security environment at both global and regional levels. The transformation of digital space through algorithmic technologies, machine learning (ML), and deep learning (DL) generates new strategic advantages while simultaneously creating asymmetrical vulnerabilities. Among the sectors most significantly influenced by AI, cybersecurity holds a distinctive position, functioning both as a target of AI-generated threats and as a domain where AI serves as a tool for defence and prevention (Brundage et al., 2018).

The use of AI in cybersecurity is characterised by a duality: on the one hand, it enables the development of sophisticated tools for anomaly detection, automated incident response, and more efficient processing of large volumes of data; on the other hand, it facilitates the emergence of new forms of cyberattacks that are autonomous, adaptive, and difficult to predict. These technological innovations fundamentally change the nature of cyber threats. Rather than relying primarily on traditional "script kiddies" (cyberattacks and computer system disruptions using pre-existing programs, scripts, or tools) or manual penetrations, contemporary threat actors increasingly employ generative models, adversarial techniques, and behavioural analyses aimed at user manipulation (Gebrehans et al., 2025).

These trends raise several fundamental questions that society must address. What specific threats and risks does AI pose in the cyber domain? How can security institutions and technological actors use artificial intelligence as a means of protection? And finally, how can the use of these technologies be normatively and strategically balanced to ensure they are safe, ethical, and socially responsible?

METHODOLOGY AND OBJECTIVE

From a methodological standpoint, this article is based on a qualitative analysis of secondary sources, including scholarly publications, articles, contributions, analytical reports, expert studies, technological platform documents, and available empirical data. The descriptive and comparative methods are primarily used to explain the issues, allowing for the identification and comparison of specific types of threats and mitigation strategies. The analytical section of the article also employs an exploratory approach, aimed at identifying trends and potential development scenarios in the field of AI-influenced cybersecurity.

The objective of this article is to scientifically explore and analyse the main threats and opportunities arising from the use of artificial intelligence in the context of cybersecurity. Particular attention is given to how AI affects security actors, from states and multinational institutions to the private sector and civil society, and to the systemic challenges that emerge as a consequence.

The chosen research framework is interdisciplinary. The author draws on knowledge related to cybersecurity, information technology, security studies, and artificial intelligence. The theoretical foundation is based on the technological determination of security threats, as well as on the concept of so-called dual-use technologies, which allows for reflecting the ambivalent nature of AI in terms of its application for both the benefit and potential detriment of security.

The article is structured into three main parts: the first focuses on the theoretical framework and an analysis of the main threats that AI poses to cybersecurity; the second part analyses the opportunities that AI offers for enhancing the protection and resilience of digital systems; the third provides a brief synthesis of AI's benefits and strategic importance. The conclusion identifies challenges for policy and research and outlines perspectives for further development in the studied area.

RESULTS AND DISCUSSION

The ongoing discussion about artificial intelligence in the security context is inherently linked to the concept of technological change as a key factor redefining the nature of threats. AI is not merely a technological tool; it increasingly acts as an active security agent with the potential to influence actor behaviour, destabilize power balances, and transform the very understanding of risk (Kundu, 2025). In this regard, the theoretical framework of "securitization of technologies" is often employed, in which new technologies, like AI, are understood both as objects of security concerns and as tools for security measures (Mügge, 2023).

From a security perspective, artificial intelligence as a phenomenon exhibits a dual-use character, serving as a tool for both defence and attack. Its distinctiveness lies in its ability to autonomously learn, adapt, and optimize its operations based on environmental feedback. This fundamentally differentiates it from traditional information technologies, which are deterministic and subject to direct human control (Brundage et al., 2018). However, such autonomy simultaneously opens up room for potential unintended consequences, misuse, and unpredictability in the behaviour of AI systems, creating a fundamental security risk, particularly when these technologies are deployed in critical infrastructures.

Therefore, from a theoretical standpoint, AI should be understood not just as a technological innovation, but also as a securitizable object that, in various contexts, acts as a threat, an actor, or a target of security policy. In the realm of cybersecurity, this perspective is especially relevant because AI reshapes the very architecture of cyber threats, including their scalability, sophistication, and adaptability (Mügge, 2023; Kundu, 2025).

THREATS POSED BY ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

As indicated earlier, the use of artificial intelligence not only brings revolutionary defensive capabilities but also introduces a broad spectrum of new, complex threats. This chapter analyses various forms of AI misuse that fundamentally change the nature of cyberattacks and expand the range of actors capable of carrying out malicious activities. This discussion addresses major security risks, starting from the generation of sophisticated malware, through adversarial attacks and deepfake technologies, to threats to critical infrastructure and the deployment of autonomous weapon systems. At the same time, it highlights structural weaknesses of AI systems, including limited transparency and susceptibility to data bias, which can have serious consequences for their trustworthy use in cybersecurity. This section aims to systematically identify and describe the main threats associated with AI deployment in the cyber domain, thereby contributing to a better understanding of their impact on the security architecture of the digital environment.

Artificial intelligence significantly enhances the effectiveness and precision of cyberattacks by enabling automated identification of system vulnerabilities, optimization of attack vectors, and dynamic adaptation of tactics based on target responses. Recent research indicates that attackers can leverage AI to develop intelligent malware capable of disguising itself, evading detection by traditional antivirus tools, and operating autonomously in response to contextual factors (Kamoun et al., 2020). AI is also applied in so-called spear-phishing

campaigns, where generative language models produce highly convincing, multilingual messages, tailored to specific targets.

With the increasing deployment of AI in defensive systems (e.g., in threat detection systems), a new type of risk emerges, known as adversarial attacks. These attacks involve manipulating inputs to cause misclassification, allowing the attacker to disrupt system functionality. Such attacks can be extremely effective because they exploit weaknesses in training datasets or in the model learning process (Lawrence, Onyemaechi, 2025). For example, a slightly modified image might be incorrectly classified as banign, even though it actually contains malicious content.

Generative AI enables the creation of realistic deepfake videos, audio recordings, and texts, which can be exploited for information operations, spreading disinformation, extortion, or discrediting political actors. This phenomenon poses a fundamental risk, especially for electoral processes, social cohesion, and trust in institutions (Chesney, Citron, 2019). In this context, cybersecurity extends beyond a purely technical issue and becomes a socio-political problem, where AI is a tool for influence and destabilization.

AI lowers technological barriers for less skilled actors, who can leverage "AI-as-a-Service" tools (e.g., exploit generators or automated vulnerability scanners) to launch attacks without needing extensive technical knowledge. This development contributes to the "democratization of cyberattacks," increasing the risk of a quantitative surge in threats and placing additional strain on defensive capabilities (Helmus, 2022).

The integration of AI into critical infrastructure systems (e.g., energy, transport, or healthcare) offers potential for optimization but simultaneously introduces new vulnerabilities. If AI models are attacked or manipulated, it can lead to real threats to public safety – for instance, through incorrect regulation of energy distribution, compromised autonomous transport control, or flawed diagnostic decisions in healthcare (ENISA, 2020).

One of the most serious threats is the deployment of artificial intelligence in weaponry, particularly in the development of Lethal Autonomous Weapon Systems (LAWS). These systems are capable of identifying, tracking, and destroying targets without human intervention, fundamentally altering existing paradigms of violence control. In the context of cybersecurity, these technologies are associated with the risk of automated military cyber operations that may escape human oversight and trigger unintended conflict escalation (Scharre, 2019). Furthermore, when autonomous systems are deployed in highly uncertain environments and without sufficiently defined rules of engagement, the risk of strategic misinterpretation

increases, potentially leading to heightened international tensions or accidental attacks on civilian targets.

AI systems are extremely sensitive to the quality and objectivity of the data they are trained on. If training data are biased, unbalanced, or contain structural distortions, models may generate inaccurate or discriminatory outputs (Barocas et al., 2019). In cybersecurity, this can result in erroneous threat assessments, false positives, or increased vulnerability to "data poisoning" attacks, where an attacker deliberately manipulates training data to influence system behaviour. At the same time, such issues undermine trust in AI-based tools for system protection, as decision-making processes may lack transparency or auditability, which is particularly problematic in sensitive domains such as the protection of public institutions or intelligence systems.

Another fundamental challenge is the "black-box" nature of many AI models, which produce outputs without providing interpretable explanation. This complicates thorough investigation of security incidents, the auditing of decisions, and the verification of output correctness. In the context of cybersecurity, this lack of transparency is especially critical when AI decisions involve attack detection, threat identification, or recommendations for incident response (Ran, 2025). In the event of an AI-based system failure, it can be practically impossible to retrospectively identify the underlying cause, which reduces accountability and legal traceability. This creates a "security asymmetry" between system users and technology developers.

OPPORTUNITIES OF UTILIZING ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

The growing capabilities of artificial intelligence (AI) not only pose threats but also create unprecedented opportunities to strengthen cybersecurity. Currently, AI is being integrated into modern defensive strategies and cyber infrastructures, where its predictive, automation, and decision-support capabilities enable more effective management of complex threats. The opportunities that AI brings can be systematized into several key areas.

One of the most significant contributions of AI to cybersecurity is its ability to detect anomalies and threats in real-time. Traditional tools, such as rule-based intrusion detection systems (IDS), are often ineffective against novel, previously unknown types of attacks. AI, particularly machine learning, can learn from historical data and identify deviations from standard system or user behaviour (Major, 2024). This allows for early warning of potential attacks, including zero-day exploits and advanced persistent threats (APTs). A typical example

is the use of deep neural networks (deep learning) in network traffic analysis, where algorithms learn to recognize suspicious patterns without relying on predefined rules. This approach significantly reduces response time while minimizing the number of false positives.

Another key area is the automation of security incident response. AI enables the development of autonomous or semi-autonomous systems that not only detect attacks but are also capable of implementing immediate mitigating measures, for instance, isolating an infected device, blocking communication with a suspicious IP address, or restoring systems from backups (Mehdi et al., 2024). Such systems are becoming indispensable, especially in environments requiring rapid response, such as financial institutions, critical infrastructure, or public administration. In this way, AI reduces dependence on the human factor, which can be overwhelmed or ineffective when facing a large number of attacks.

Artificial intelligence also plays a key role in predictive analytics, which involves anticipating the development of security situations based on past incidents, emerging trends, and attacker behaviour patterns. By collecting and processing large volumes of data – from system logs and network traffic to open-source intelligence (OSINT) – AI tools can predict potential cyberattacks, identify vulnerabilities in real time, and provide recommendations for optimizing security policies (PAN, 2024). In this context, AI is increasingly embedded in Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) platforms. Machine learning-enhanced systems not only improve incident handling efficiency but also enable a deeper understanding of threat contexts and the dynamic adaptation of defensive mechanism.

The deployment of AI in the protection of critical infrastructure, such as energy grids, transportation systems, water management facilities, and healthcare services, is of particular importance. These systems are increasingly connected to the internet and are thus becoming targets of sophisticated attacks. AI enables continuous system monitoring, detection of anomalies in performance or integrity, and automatically initiate recovery processes (Crichton et al., 2024). AI's ability to integrate data from heterogeneous sensors, identify predictive indicators of system failure, and contribute to the development of proactive security architectures is also crucial, enhancing the overall resilience of systems against both external and internal threats.

Finally, AI offers tools for improving cyber literacy and effectively tailoring security training for employees. Using personalized algorithms, AI can identify weaknesses in user behaviour, simulate realistic attacks (e.g., phishing campaigns), and generate adaptive educational modules that raise awareness levels and reduce the risk of human error (Kumar,

2024). In this respect, AI contributes not only to the technical security of systems but also to the development of a security-conscious culture as an essential component of a comprehensive approach to cybersecurity protection.

BRIEF SYNTHESIS OF AI'S BENEFITS AND STRATEGIC IMPORTANCE

Based on the above, it can be concluded that just as cybersecurity has progressively become an integral component of overall security assurance (Ivančík, Kazanský, 2024), artificial intelligence is gradually becoming an indispensable element of modern cyber defence. Its benefits are diverse, ranging from proactive threat and anomaly detection, automated incident response, and predictive analytics to critical infrastructure protection and the enhancement of security awareness.

AI enables the transformation of cybersecurity from a predominantly reactive model into a proactive and adaptive one, thereby increasing not only the effectiveness of protection mechanisms but also the ability of systems to respond to new and previously unknown threats (Pipeline, 2023). Importantly, these capabilities are not merely technological innovations; they also have geopolitical, strategic, and systemic implications - especially for state authorities, security forces, the defence industry, and public services sector.

At the same time, however, it is evident that the deployment of AI alone is insufficient without a robust normative and ethical framework and without the parallel strengthening of human resilience. Artificial intelligence is only as effective as its integration into the overall security ecosystem, including organizational culture, legislative frameworks, and international cooperation.

Therefore, it is crucial not only to invest in AI technologies but also to create policies that support the responsible, transparent, and effective use of AI tools for protecting cyberspace (Nagel et al., 2025). This requires a multidisciplinary approach involving technologists and security experts, as well as legal professionals, ethicists, political leaders, and international organizations. Collaboration among these actors is essential for establishing regulatory frameworks that ensure AI serves as a means of protection and stability rather than a driver of destabilization or conflict escalation.

In the long term, the strategic balance in cyberspace will increasingly depend on the ability of states and alliances to combine technological capabilities with a trustworthy and values-based approach to AI governance and deployment. In this context, the European model of trustworthy AI comes into play, emphasizing accountability, auditability, and the protection

of fundamental rights, which can serve as a counterbalance to less transparent and repressively oriented approaches in authoritarian regimes (Floridi, 2021).

Ultimately, the strategic importance of artificial intelligence lies not only in its technical potential but also in its capacity to shape power balances, influence actor behaviour, and define the boundaries of cyber sovereignty. In this context, it is imperative for states and institutions not only to invest in the development of AI technologies but also to ensure their responsible integration within a values-consistent and democratic security order.

CONCLUSION

The growing importance of artificial intelligence in cybersecurity represents one of the most significant technological and strategic shifts of recent years. This article has demonstrated that AI has become an indispensable component of modern defence mechanisms against increasingly sophisticated and complex threats in the digital domain. It allows not only for faster and more accurate detection of cyberattacks but also for proactive prediction and adaptive responses to new and often previously unknown types of threats.

On the other hand, however, the use of AI also brings substantial risks, including its potential misuse for malicious purposes, the creation of autonomous weapon systems, and reduced transparency in decision-making processes. These risks are not only technical but also ethical, legal, and geopolitical in nature, requiring comprehensive regulation, multilateral cooperation, and an emphasis on democratic oversight and accountability.

A key finding is that artificial intelligence cannot be treated as a neutral instrument; rather, it functions as a formative force that reshapes the balance of power, the distribution of risks, and the security strategies of actors. Therefore, the effective integration of AI in cybersecurity must be grounded in principles of responsibility, robustness, explainability, and human control.

From a practical perspective, this implies the need for sustained investment not only in the development and deployment of AI technologies but also in the establishment of regulatory frameworks, international standards, and mechanisms for monitoring their implementation. Equally important is the strengthening of interdisciplinary research at the intersection of computer science, law, ethics, and security studies.

With regard to future research, attention should be directed toward three main areas:

1. Examining the impacts of autonomous AI-driven decisions on strategic stability and cyber retaliation dynamics.

2. Developing mechanisms to ensure transparency and auditability of AI systems used for security purposes.

3. Evaluating the effectiveness and international compatibility of existing regulatory frameworks governing AI and cybersecurity.

The future of cybersecurity will largely depend on how quickly and responsibly society can respond to the challenges associated with the widespread adoption of artificial intelligence. Gaining supremacy in this field will not merely confer a technological edge but will also translate into strategic leverage in an increasingly digitized global environment. Artificial intelligence thus becomes not only a tool for security but also an object of power, the mastery of which will shape the political, economic, and security standing of states and actors in a multipolar world. At the same time, it's clear that effectively managing AI's potential requires synergy among state policies, academic research, the technological sector, and civil society. Only a comprehensive and inclusive approach that integrates technical, ethical, legislative, and geopolitical aspects can ensure that artificial intelligence becomes a tool for strengthening cybersecurity and not a source of its weakening.

LITERATURE AND INFORMATION SOURCES USED

1. BAROCAS, S. – HARDT, M. – NARAYANAN, A. (2023). *Fairness and Machine Learning. Limitations and Opportunities*. Boston: Massachusetts Institute of Techno-logy Press, 2023. 340 p. ISBN 978-0-262-37652-5.

2. BRUNDAGE, M. et al. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. In *Centre for the Study of Existential Risk, University of Cambridge*, 2018. [online]. [cit. 2025-07-11]. DOI: 10.48550/arXiv.1802.07228.

3. CRICHTON, K. a kol. (2024). Securing Critical Infrastructure in the Age of AI. In: *Center for Security and Emerging Technology*, 2024. [online]. [cit. 2025-07-14]. Available at: https://cset.georgetown.edu/publication/securing-critical-infrastructure-in-the-age-of-ai/.

4. CHESNEY, R. – CITRON, D. K. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. In *California Law Review*, 2019, Vol. 107, No. 6, pp. 1753-1820. ISSN 0008-1221. DOI: 10.15779/Z38RV0D15J.

5. ENISA. (2020). Artificial Intelligence Cybersecurity Challenges. In *European Union Agency for Cybersecurity*, 2022. [online]. [cit. 2025-07-13]. Available at: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges.

6. FLORIDI, L. (2021). *Ethics, Governance, and Policies in Artificial Intelligence*. Oxford: Oxford Internet Institute, University of Oxford, 2021. 392 p. ISBN 978-3-030-81906-4. DOI: 10.1007/978-3-030-81907-1.

7. GEBREHANS, G. – ILYAS, N. – ELEDLEBI, K. (2025). Generative Adversarial Networks for Dynamic Malware Behavior: A Comprehensive Review, Categorization, and Analysis. In: *IEEE Transactions on Artificial Intelligence*, 2025, pp. 1-23. ISSN 2691-4581. [online]. [cit. 2025-07-11]. DOI: 10.1109/TAI.2025.3537966.

8. HELMUS, T. C. (2022). Artificial Intelligence, Deepfakes, and Disinformation. In *RAND Corporation*, 2022. [online]. [cit. 2025-07-13]. Available at: https://www.rand.org/pubs/perspectives/PEA1043-1.html.

9. LAWRENCE, S. I. – ONYEMAECHI, E. O. (2025). Adversarial Attacks and Defenses in AI Systems: Challenges, Strategies, and Future Directions. In: *International Journal of Research and Innovation in Applied Science,* 2025, Vol. 10, No. 2, pp. 996-1022. ISSN 2454-6194. [online]. [cit. 2025-07-12]. DOI: 10.51584/IJRIAS.2025.10060075.

10. IVANČÍK, R. – KAZANSKÝ, R. (2023). Quo Vadis Humanity? A View of Some Current Global Security Threats and Challenges. In: *Security Science Journal*, 2023, Vol. 4, No. 1, pp. 68-82. ISSN 2737-9493. [online]. [cit. 2025-07-12]. DOI: 10.37458/ssj.4.1.5.

11. IVANČÍK, R. – KAZANSKÝ, R. (2024). Cyber Security as a Contemporary Security Challenge. In: *Contemporary Security Challenges and Strenghtnening the Resilience of the Countries of Souhtwest Europe – Conference Proceedings from International Scientific Conference*. Ohrid, 2024, pp. 61-70. ISSN 2671-3624. [online]. [cit. 2025-07-12]. DOI: 10.20544/ICP.9.1.24.P05.

12. IVANČÍK, R. (2021). A Treatise on the Paradigm of Seurity Theory. In: *Auspicia*, 2021, Vol. 18, No. 2, pp. 78-93. ISSN 2464-7217. [online]. [cit. 2025-07-12]. DOI:10.36682/a_2021_2_5.

13. KAMOUN, F. – ESSEGHIR, M. A. – BAKER, T. (2020). AI and machine learning: A mixed blessing for cybersecurity. In: *International Symposium on Networks, Computers and Communications*, 2020, pp. 1-7. ISBN 978-1-7281-5628-6. [online]. [cit. 2025-07-13]. DOI: 10.1109/ISNCC49221.2020.9297323

14. KUMAR, A. (2024). The Role of Artificial Intelligence in Digital Literacy Training. In: *International Journal of Research Publication and Reviews*, 2024, Vol. 6, No. 4, pp. 63-69. ISSN 2582-7421. [online]. [cit. 2025-07-14]. Available at: https://ijrpr.com/uploads/V6ISSUE4/IJRPR43584.pdf.

15. KUNDU, R. (2025). AI Risks: Exploring the Critical Challenges of Artificial Intelligence. In: *Lakera AI Security*, 2025. [online]. [cit. 2025-07-12]. Available at: https://www.lakera.ai/blog/risks-of-ai.

16. MAJOR, K. (2024). The Impact of Artificial Intelligence and Machine Learning on IAM. In: *Major Key Tech's*, 2024. [online]. [cit. 2025-07-14]. Available at: https://www.majorkeytech.com/blogs/impact-of-ai-machine-learning-on-iam.

17. MEHDI, H. – FAOUZI, J. – BOUHOULA, A. (2024). Cyber Security within Smart Cities: A Comprehensive Study and a Novel Intrusion Detection-Based Approach. In: *Computers, Materials & Continua*, 2024, Vol. 81, No. 1, pp. 393-409. ISSN 1546-2218. DOI: 10.32604/cmc.2024.054007.

18. MÜGGE, D. (2023). The securitization of the EU's digital tech regulation. In: *Journal of European Public Policy*, 2025, Vol. 30, No. 7, pp. 1431–1446. 1466-4429. [online]. [cit. 2025-07-13]. Available at: https://doi.org/10.1080/13501763.2023.2171090.

19. NAGEL, J. – LINDEGAARD, M. – GRAABAK, J. (2025). Strengthening AI trustworthiness. In: *Centre for Future Generations*, 2025. [online]. [cit. 2025-07-14]. Available at: https://cfg.eu/strengthening-ai-trustworthiness/.

20. PAN. (2024). What are Predictions of Artificial Intelligence (AI) in Cybersecurity? In: *Palo Alto Networks*, 2025. [online]. [cit. 2025-07-14]. Available at: https://www.paloaltonetworks.com/cyberpedia/predictions-of-artificial-intelligence-ai-in-cybersecurity.

21. PIPELINE, I. (2023). Artificial Intelligence in Cybersecurity. Transforming Cyber Defence Mechanism. In: *Pipeline Incorporation*, 2023. [online]. [cit. 2025-07-14]. Available at: https://www.ppln.co/en/posts/ai-in-cybersecurity.

22. RAN, X. (2025). A Systems Approach to Shedding Sunlight on AI Black Boxes. In: *Hofstra Law Review*, 2025. Vol. 53, No. 3, pp. 1-47. ISSN 0091-4029. [online]. [cit. 2025-07-13]. DOI: 10.2139/ssrn.4966957.

23. SCHARRE, P. (2019). *Armáda strojov. Autonómne zbrane a budúcnosť vojny*. Bratislava: Ikar, 2019. 488 p. ISBN 978-80-551-6548-6.

ADDRESS & ©

JUDr. Jana ZACHAR KUCHTOVÁ, PhD.
Akadémia Policajného zboru
Sklabinská 1
817 35 Bratislava, Slovenská republika
jana.kuchtova@akademiapz.sk

BEZPEČNOST • SAFETY

DOI: 10.36682/a_2025_2_2

SECURITY AND STRATEGIC STUDIES WITHIN INTERNATIONAL RELATIONS: THEORETICAL DELINEATION, DEVELOPMENTAL TRAJECTORIES, AND CONTEMPORARY CHALLENGES

Bezpečnostné a strategické štúdie v rámci medzinárodných vzťahov: teoretické vymedzenie, vývojové trajektórie a súčasné výzvy

Radoslav IVANČÍK

Nitra, Slovak Republic

ABSTRACT: The article examines the evolving relationship between strategic and security studies within the broader framework of international relations. These subfields, originally intertwined during the Cold War, have undergone substantial theoretical and methodological differentiation in response to changing dynamics of global and regional security developments. The article identifies strategic studies as a subfield focused on how actors – primarily states – use military means to achieve political objectives, whereas security studies are understood as a broader, interdisciplinary field dealing with both military and non-military threats. Through historical-process, content and comparative analysis, the author traces conceptual shifts in the understanding of security, highlighting the growing relevance of hybrid threats, technological advances and renewed prominence of conventional warfare. The author argues for the complementary use of both strategic and security studies in contemporary research and policymaking, emphasizing the need for a pluralistic, dynamic and practice-oriented security science. In conclusion, the article highlights the normative and epistemic challenges that society faces and calls for integrated research frameworks capable of addressing strategic uncertainty, instability, and transformations in global power structures.

Key words: Security studies – strategic studies – international relations – security science – interdisciplinary research

ABSTRAKT: Článok skúma vyvíjajúci sa vzťah medzi strategickými a bezpečnostnými štúdiami v širšom rámci medzinárodných vzťahov. Tieto podoblasti, ktoré boli pôvodne prepojené počas éry studenej vojny, prešli podstatnou teoretickou a metodologickou diferenciáciou v reakcii na meniacu sa dynamiku vývoja globálnej a regionálnej bezpečnosti. Článok identifikuje strategické štúdie ako podoblasť zaoberajúcu sa spôsobmi, akými aktéri – predovšetkým štáty – používajú vojenské prostriedky na dosiahnutie politických cieľov, zatiaľ čo bezpečnostné štúdie sú koncipované ako širší, interdisciplinárny prístup zaoberajúci sa vojenskými aj nevojenskými hrozbami. Prostredníctvom historicko-procesnej, obsahovej a porovnávacej analýzy autor sleduje koncepčné posuny v chápaní bezpečnosti, pričom zdôrazňuje rastúci význam vzostupu hybridných hrozieb, technologického pokroku a návratu konvenčného boja. Autor argumentuje za komplementárne využitie oboch podoblastí v súčasnom výskume a tvorbe politík, pričom zdôrazňuje potrebu pluralistickej, dynamickej a prakticky orientovanej bezpečnostnej vedy. Na záver zdôrazňuje normatívne a epistemické výzvy, ktorým spoločnosť čelí, a vyzýva na integrované výskumné rámce schopné reagovať na strategickú neistotu, nestabilitu a globálne mocenské transformácie.

Kľúčové slová: Bezpečnostné štúdiá – strategické štúdiá – medzinárodné vzťahy – bezpečnostná veda – interdisciplinárny výskum

INTRODUCTION

The relationship between strategic and security studies represents one of the most crucial, yet theoretically and methodologically complex, lines of internal differentiation within the discipline of International Relations. From its institutional emergence in the aftermath of the Second World War to its current paradigmatic plurality, academic security research faces fundamental questions regarding its subject matter, normative foundations, and the purpose of scientific inquiry. Strategic and security studies were initially indistinguishable and closely linked to the military thinking of great powers in the bipolar international system of the Cold War era. Following the end of the Cold War, however, substantial revisions of theoretical foundations led to the differentiation and redefinition of both fields within the broader security discourse. In this context, a new academic consensus gradually emerged, according to which security studies constitute a broader analytical framework encompassing both military and non-military threats, while strategic studies are understood as its military-oriented subfield (Jurčák & Trebula, 2017).

Although earlier scholarly perspectives attempted to equate these fields (Haftendorn, 1991; Walt, 1991), developments in the last three decades have clearly demonstrated that differentiation is not only justified but also heuristically productive. The rise of new, particularly asymmetric security threats such as cyberattacks on public and private computer networks and systems, terrorism, financial, economic, energy, and environmental crises (Tvaronavičienė, 2024; Rožňák & Juríček, 2014; Majchút, 2024), pandemic risks, or hybrid forms of conflict (Andrassy & Ondruš, 2024; Dušek & Kavan, 2024), does not preclude, but rather emphasizes the need to preserve the classical strategic dimension in security thinking. Echevarria (2021) adds that ongoing military conflicts reaffirm the enduring importance of strategy as a critical link between political objectives and the use of military means.

METHODOLOGY AND OBJECTIVE

The objective of this article is to analyse the development and relationship between security and strategic studies within the discipline of International Relations, to identify their specifics and transformations over time, and to highlight the need for their complementary application in contemporary security research. Rather than proposing new definitions of either

field, the article seeks to illustrate their developmental trajectories, shifts within academic discourse, and their ability to respond to a dynamically changing global and regional security environment, as well as to ongoing transformations in international relations.

From a methodological perspective, the author employs an interdisciplinary research approach that combines content analysis, comparative analysis, and historical process tracing with elements of conceptual reconstruction and paradigmatic comparison. Drawing on the works of established domestic and international scholars, the study examines shifts in the understanding of security in response to evolving international environment. The analytical-synthetic and process-analytical methods allow for the identification of causal links between key historical events and transformations in theoretical discourse, with particular attention to how specific concepts gain or lose prominence depending on the prevailing security context.

The analytical framework also incorporates a contextual epistemology of security, which conceptualizes security as a construct shaped by the social, political, and ideological structures of a given era. In analytically distinguishing between security and strategic studies, the author draws on their institutional, thematic, and methodological characteristics. Based on the research findings, the article concludes by offering interpretive insights into the significance of both types of studies for contemporary security science within the context of a multipolar, unstable, uncertain, and value-fragmented international environment.

RESULTS AND DISCUSSION

Security and strategic studies represent two important directions of academic inquiry, closely intertwined with developments in security, international relations, and broader geopolitical transformations throughout the 20th and 21st centuries. Despite their strong interconnection, particularly during the Cold War, these research areas cannot be understood as identical, as their subject matter, research methods, and even institutional embeddedness have diversified over time. The evolution of both sub-disciplines reflects not only the broader trend of pluralization of International Relations theories but also the transition from a state-centric to a multi-dimensional and multi-actor model of security, and the growing importance of interdisciplinarity in security research.

HISTORICAL AND THEORETICAL DELINEATION OF SECURITY AND STRATEGIC STUDIES

In the early post-World War II period, security and strategic studies largely overlapped. Both fields emerged as a response to the urgent need to intellectually process new global threats, particularly the prospect of ballistic missile and nuclear warfare between the two dominant, antagonistic military-political blocs of the time (the North Atlantic Treaty Organization and the Warsaw Pact), and to provide analytical frameworks for the formulation of military-political strategies (Küpeli, 2021). During this period, several key institutions were established, such as the RAND Corporation, the Harvard Center for International Affairs, and the Institute for Strategic Studies, which formed the core of the so-called golden age of strategic studies. Key themes included deterrence, the balance of power, total war strategy, and the concept of "grand strategy" (Walt, 1991; Paret et al., 2010).

Strategic studies were defined as "a field of research concerned with the ways in which actors – primarily states – use military means to achieve political ends" (Evans & Newnham, 1998, p. 518). Their core focus lay in the study of military power, defence planning, operational doctrines, and the relationship between politics and war. These studies were largely influenced by realist and neo-realist theoretical frameworks, drawing inspiration from Carl von Clausewitz's classical conception of strategy, which viewed war as the continuation of state policy by other means (Clausewitz, 2020).

Security studies, understood as a distinct field, began to emerge more clearly only toward the end of the Cold War. It is defined as "a sub-field of international relations that deals with the elucidation of the concept of security, its implementation in foreign policy formulation, and its subsequent effect on structures and processes in world politics" (Evans & Newnham, 1998, p. 496). This approach focused on clarifying how security is conceptualized, who or what constitutes its referent object, and which means are considered legitimate for its provision.

During the Cold War, the two disciplines significantly overlapped, largely because security studies focused predominantly on military threats, particularly the risik of potential nuclear conflict between the United States of America (USA) and the former Union of Soviet Socialist Republics (USSR) (Suchý, 2003). In this context, Walt defined security studies as "the study of the threat, use, and control of military force" (Walt, 1991, p. 212). This narrow understanding contributed to the frequent treatment of security and strategic studies as essentially synonymous.

The collapse of the bipolar international system in the late 1980s and early 1990s, however, necessitated a reassessment of this conception of security. New challenges emerged,

including irregular mass migration, climate change, failing states, rogue states, transnational organized crime, and terrorism, phenomena that clearly transcend the scope of military solutions. As a result, security studies could no longer rely solely on a state-centric and military-technical approach (Kolodziej, 1992). This shift led to the emergence of the so-called broadened concept of security, which encompasses security concerns extending beyond traditional military frameworks. In this context, scholars of the Copenhagen School introduced the concept of securitization, arguing that security should be understood as not an objective condition but as an intersubjective discourse (Buzan et al., 1998).

The result of this transformation is a consensus that security studies constitute a more comprehensive analytics framework, within which strategic studies function as a specialized and predominantly military-oriented sub-discipline. Jurčák and Trebula (2017) point out that the achieved consensus between so-called traditionalists and wideners regarding the need to distinguish between these two areas constitutes a significant epistemological advance. Contemporary understanding thus reflects a dual structure: (a) security studies as a multidisciplinary field examining a wide range of threats, and (b) strategic studies as an analytical framework primarily focused on military tools for ensuring security.

This distinction is important not only from a theoretical perspective but also, more importantly, for the practical application of knowledge in political and security decision-making. As developments since 2014 (the illegal Russian annexation of Crimea) and especially since 2022 (Russia's military invasion of Ukraine) demonstrate, the importance of military strategy has once again become pronounced, even in an environment characterized by growing hybrid and asymmetric threats. This development underscores the dynamic and complementary relationship between security studies and strategic studies and highlight their continued importance for understanding contemporary international security realities.

PARADIGMATIC SHIFTS AFTER THE END OF THE COLD WAR

The end of the Cold War constituted a fundamental turning point in both political reality and the scholarly understanding of security. The collapse of the bipolar system and the disappearance of the immediate threat of nuclear conflict between the superpowers led many scholars to question whether security and strategic studies still possessed a clearly defined subject of inquiry. At the time, many researchers assumed that these research areas would either disappear altogether or be absorbed into broader areas such as peace or development studies (Suchý, 2003). However, empirical developments demonstrated the opposite: both security and

strategic studies underwent processes of redefinition, diversification, and a shift towards a broader, more comprehensive understanding of security.

Within the academic debates of the 1990s, three basic approaches emerged concerning the future of security studies: (a) the preservation of the status quo, (b) moderate reform, and (c) radical reform (Baldwin, 1995, pp. 133-134). Walt, a leading representative of the realist tradition, argued in favour of maintaining a narrow conception of security studies focused primarily on the study of military force, its use, and control. He warned that "excessive expansion of their scope could lead to a loss of coherence and scientific analytical rigor" (Walt, 1991, p. 213). At the same time, however, he acknowledged the need to address new challenges, particularly the redefinition of national interests, the role of grand strategy, the interaction between domestic politics and security, and the security implications of economic globalization (Walt, 1991, pp. 224-227).

Advocates of moderate reform, such as Haftendorn (1991), supported expanding attention to previously marginalized regions and topics, including security dynamics in Asia or in developing countries. According to this approach, strategic studies were expected to adapt to the new, transformed environment while maintaining their analytical framework grounded in military-political logic.

Radical reform, represented by scholars such as Buzan et al. (1998), Kolodziej (1992), and Kegley (1993), rejected the traditional state-centric and military-deterministic conception of security. Buzan, Wæver, and de Wilde (1998) introduced a new analytical framework, known as the Copenhagen School, which expanded the security discourse to encompass five sectors: military, political, economic, environmental, and societal. Within this framework, security is not merely an objective state but a social construct that emerges through the process of "securitization," whereby a particular phenomenon is framed as an existential threat, thereby justifying the adoption of exceptional measures, including the potential use of military force.

According to Kolodziej (1992), security studies must also address issues such as human rights, humanitarian crises, global justice, and the governance of common goods. In this context, security research transforms into an interdisciplinary platform, integrating insights from political science, economics, sociology, demography, ecology, and other scientific fields.

As a result of this evolution, security studies developed into a broader framework for security research, whereas strategic studies retained a narrower, predominantly military focus. This differentiation gained general acceptance across both camps – traditionalists and reformists alike – thereby contributing to the stabilization of both sub-disciplines within

international relations (Jurčák & Trebula, 2017). At the same time, however, it highlighted the need for a more nuanced understanding of how these fields can be used complementarily.

Evidence that strategic studies remain highly relevant rather than a relic of the past, can be found in developments in the global and regional security environment since 2001. Events such as the terrorist attacks in the United States (9/11), military interventions in Afghanistan and Iraq, Russian aggression against Ukraine (2014, 2022), and growing geopolitical tensions in the Indo-Pacific region demonstrate that military force and strategic planning continue to play a key role in safeguarding national and alliance interests (Kazanský & Cséfalvay, 2023; Echevarria, 2021).

At the same time, these events underscore the need for a reform of strategic thinking in response to new phenomena, including hybrid threats, information and psychological operations, cyberattacks, and asymmetric conflicts. As the Clausewitz-inspired Colin Gray (1999) emphasizes, strategy is timeless in essence – the link between political objectives and military means remains unchanged, even as its content and forms evolve.

In this context, a pluralistic understanding of security knowledge has emerged, recognizing multiple, equally valid analytical frameworks – ranging from classical strategic realism to constructivist, humanitarian, postcolonial, and feminist approaches. Despite their differences, these perspectives share a common goal: to understand existing and emerging threats, risks, and challenges, and to identify opportunities for maintaining peace and stability in a dynamically changing reality.

CONTEMPORARY CONTEXT AND METHODOLOGICAL CHALLENGES IN SECURITY AND STRATEGY RESEARCH

The contemporary international security environment is characterized by increasing complexity, interconnectedness, and instability. Multipolarity, the resurgence of power politics, technological breakthroughs, climate change, risks associated with energy transitions, persistent conflicts, and the emergence of hybrid threats (Koudelka, 2016; Ivančík – Kazanský, 2023; Dirma et al., 2024) create conditions that extend beyond the scope of classical security theories. In this context, there is a heightened need for innovative approaches to security that integrate insights from both security and strategic studies into a dynamic, applicable, and pluralistic research framework (Buzan & Hansen, 2009; Piwowarski et al., 2024; Kazanský & Cséfalvay, 2023).

Strategic studies are currently regaining both academic and political prominence. Their significance had been questioned, particularly during the period of "liberal peace" after the Cold

War, it was widely assumed that military force would yield to diplomatic, economic, and legal instruments. This assumption, however, proved premature. Developments in recent years, particularly since the outbreak of the war in Ukraine, demonstrate that strategy, military capability, and defence planning remain crucial for the survival of states and the preservation of international order (Echevarria, 2021; Nečas & Procházka, 2020).

Although strategy remains at the core of strategic studies, its content and character have fundamentally evolved. The classical, state-centric, and linear conception of conflicts has been replaced by complex scenarios involving both state and non-state actors, cyberspace, information manipulation, economic coercion, and the misuse of artificial intelligence (EC, 2024; Zachar Kuchtová, 2024). This "postmodern strategy" is no less significant than its predecessor, yet it is more difficult to grasp, multi-dimensional, and less predictable. As Gray (1999) cautions, strategy must simultaneously be abstract and applied, analytical and pragmatic, military and political.

Within security studies, the debate over appropriate methodological approaches to security research (Ivančík, 2021a, 2021b) has been deepening. The plurality of approaches – from positivism, through interpretative, to critical and post-structuralist frameworks – creates a robust, yet challenging foundation for the analytical integration of knowledge. While strategists have traditionally favoured analytical models, security theorists increasingly employ discursive and contextual methods (Baldwin, 1995; Buzan & Hansen, 2009). This divergence creates a methodological asymmetry between the two disciplines, which can hinder their complementarity.

Another challenge is the redefinition of security concepts in response to accelerating technological change. Modern technologies, such as drones, cyber weapons, autonomous systems, quantum computing, and artificial intelligence, fundamentally change the character of force, methods of conflict, and the logic of deterrence. Classical terms like war, power, deterrence, and sovereignty acquire new meanings, requiring their reconceptualization not only empirically but also theoretically. For instance, the concept of "strategic autonomy" in European discourse builds on the traditional understanding of independent military decision-making, while simultaneously encompassing a broader framework of industrial, economic, technological, and political independence.

In this context, multidisciplinary is gaining increasing importance. Contemporary security research requires insights from security, military, and political sciences, international relations, philosophy, ethics, law, economics, sociology, as well as from technology and media studies. This creates space for a new model of security science that is not only descriptive but

also normative, critical, and application-oriented. Jurčák and Trebula (2017) highlight that the greatest challenge in current research lies is finding a balance between analytical precision and practical relevance.

In the light of these considerations, it is desirable to understand security and strategic studies as complementary and mutually reinforcing. While security studies provide a broader, political-societal framework for understanding threats and risks, strategic studies allow for a more detailed understanding of the specifics of using military force in specific operational and political contexts. Their integration is necessary for comprehending the complexity of the current security environment – from hybrid conflicts and great power competition to new forms of violence and coercion.

CONCLUSION

Over recent decades, security and strategic studies have undergone significant development, reflecting profound changes in the international security environment, as well as broader epistemological and methodological shifts within the discipline of International Relations. From a narrow focus on the military dimension during the Cold War, security discourse gradually expanded to encompass new types of threats and analytical frameworks, with security studies establishing itself as a broad, pluralistic, and interdisciplinary field of research. Throughout this evolution, strategic studies have retained their identity as a militarily oriented sub-discipline, which remains indispensable for examining phenomena related to the use of force, military planning, and strategy in the pursuit of achieving political objectives.

Regarding the research question, namely, how the relationship between security and strategic studies has formed and evolved, and what its current state is, it can be concluded that these disciplines have transitioned from a state of almost complete overlap to a stabilized differentiation. This distinction allows for their effective methodological and practical application. Security studies provide a comprehensive framework for understanding various types of threats, from military to environmental, social, energy, and technological, while strategic studies specialize in the use of military force, strategic thinking, and planning. However, both types share a common objective: to understand the dynamics of power, conflict, and security in an increasingly complex and rapidly changing world.

The current evolution of the international order, characterized by multipolarity, power rivalry, fragmentation, rapid technological changes, instability, and the resurgence of conventional and hybrid threats, demonstrates that neither security nor strategic studies have lost their relevance. On the contrary, their analytical interconnection is crucial for understanding

the new generation of conflicts and challenges facing human society. As illustrated by cases like the war in Ukraine, the rising power of China, or the destabilization of the global order, the ability to think strategically and act securely is decisive for the survival and prosperity of states.

However, research in these areas faces multiple challenges. These primarily include methodological fragmentation, tensions between academic autonomy and political demand, the persistence of Western-centric frameworks, and the necessity to respond to accelerating technological innovations. Under these conditions, it is essential to seek new forms of interdisciplinary knowledge integration, enhance research applicability, and strike a balance between normative vision and analytical precision.

In conclusion, security and strategic studies, despite their distinct foci, represent complementary pillars of contemporary security research. Their mutual interconnectedness, dialogue, and synergy are prerequisites not only for understanding 21st-century security challenges but also for informing the development of effective, efficient, responsible, and sustainable security policies. In an era marked by the return of conventional warfare, the proliferation of hybrid operations, the weakening of international institutions, and accelerated technological advancement, the need for systematic, theoretically grounded, and strategically oriented research has never been greater.

Security studies currently function as an analytical framework that enables the identification and interpretation of a broad spectrum of threats, ranging from military to environmental, socio-economic, energy, cyber, and pandemic threats, while also addressing normative concerns such as human security, political accountability, and justice. Strategic studies, conversely, remain essential for understanding the operational, tactical, and power-related aspects of force employment within an increasingly complex and unstable international environment. The relationship between these fields is thus not hierarchical but horizontal: they represent two complementary analytical perspectives that, when integrated, provide deeper and more precise insights.

For the future development of both fields, critical factors will include methodological integration, responsiveness to emerging threats, and the willingness to transcend established frameworks in favour of appropriate interdisciplinary solutions. It will also be necessary to overcome epistemological barriers between classical strategic approaches and constructivist or postcolonial perspectives within security studies, thereby laying the foundation for a more inclusive, dynamic, and practically oriented security science. Given the complexity of the contemporary world, merely describing security threats is no longer sufficient; the challenge

lies in understanding them within the context of global power shifts, (geo)political instability, and the erosion of the normative frameworks or the liberal order.

For this reason, future research must be guided not only by the pursuit of scientific rigor but also by a profound responsibility to society. The role of strategic and security studies extends beyond analysing conflicts and understanding their causes. It involves contributing critically to their prevention, the de-escalation of tensions, and the effective and efficient resolution of security challenges. This dual role underpins not only their academic relevance but also their practical, societal significance, serving as instruments of reflection, analysis, and guidance in times of strategic uncertainty.

LITERATURE AND INFORMATION SOURCES USED

1. ANDRASSY, V. – ONDRUŠ, M. (2024). Pohľad na problematiku hybridnej vojny po anexii Krymského polostrova. In: *Vojenské reflexie*, 2024, vol. 19, no. 1, pp. 24-36. ISSN 1336-9202. [online]. [cit. 2025-07-14]. . Available at: https://doi.org/10.52651/vr.a.2024.1.24-36.

2. BALDWIN, D. A. (1995). *Security Studies and the End of the Cold War*. In: *World Politics*, 1995, vol. 48, no. 1, pp. 117-141. ISSN 0043-8871. [online]. [cit. 2025-07-14]. Available at: https://doi.org/10.1353/wp.1995.0001.

3. BUZAN, B. – HANSEN, L. (2009). *The Evolution of International Security Studies*. Cambridge: Cambridge University Press, 2009. 400 s. ISBN 978-0-521-87393-2.

4. BUZAN, B. – WÆVER, O. – DE WILDE, J. (1998). *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998. 239 s. ISBN 978-1-55587-784-2.

5. CLAUSEWITZ, C. (2020). *O válce.* Praha: Leda, 2020. 984 s. ISBN 978-80-7335-672-9.

6. DIRMA, V. – OKUNEVIČIŪTĖ NEVERAUSKIENĖ, L. – TVARONAVIČIENĖ, M. – DANILEVIČIENĖ I. – TAMOŠIŪNIENĖ, R. (2024). The Impact of Renewable Energy Development on Economic Growth. In *Energies*, 2024, vol. 17, no. 24, art. 6328. ISSN 1996-1073. [online]. [cit. 2025-07-16]. Available at: https://doi.org/10.3390/en17246328.

7. DUŠEK, J. – KAVAN, Š. (2024). Dezinformace jako součást hybridních hrozeb – česko-slovenský pohled. In: *Auspicia*, 2024, vol. 21, no. 1, pp. 7-25. ISSN 2464-7217. DOI: 10.36682/a_2024_1_1.

8. EC. (2024). Strategic communication and countering foreign information manipulation and interference. In: *European Commission*, 2024. [online]. [cit. 2025-07-14]. Available at: https://commission.europa.eu/topics/countering-information-manipulation_en.

9. ECHEVARRIA, A. J. (2021). *War's Logic: Strategic Thought and the American Way of War*. Cambridge: Cambridge University Press, 2021. 300 p. ISBN 978-1-107-46501-5.

10. EVANS, G. – NEWNHAM, J. (1998). *The Penguin Dictionary of International Relations*. London: Penguin Books, 1998. 640 s. ISBN 978-0-14-051397-2.

11. GRAY, C. S. (1999). *Modern Strategy*. Oxford: Oxford University Press. 495 p. ISBN 978-0-19-878251-3.

12. HAFTENDORN, H. (1991). The Security Puzzle: Theory Building and Discipline-Building in International Security. In: *International Studies Quarterly*, 1991, vol. 35, no. 1, pp. 3-17. ISSN 0020-8833. [online]. [cit. 2025-07-14]. Available at: https://doi.org/10.2307/2600386.

13. IVANČÍK, R. – KAZANSKÝ, R. (2023). Quo Vadis Humanity? A View of Some Current Global Security Threats and Challenges. In: *Security Science Journal*, 2023, vol. 4, no. 1, pp. 68-82. ISSN 2737-9493. [online]. [cit. 2025-07-16]. Available at: https://doi.org/10.37458/ssj.4.1.5.

14. IVANČÍK, R. (2021a). Security Theory: Security as a Multidimensional Phenomenon. In: *Vojenské reflexie*, 2021, roč. 16, č. 3, s. 32-53. ISSN 1336-9202. [online]. [cit. 2025-07-16]. Available at: https://doi.org/10.52651/vr.a.2021.3.32-53.

15. IVANČÍK, R. (2021b). Treatise on Postulates of Security Theory. In: *Security Science Journal*, 2021, roč. 2, č. 1, s. 108-124. ISSN 2737-9493. [online]. [cit. 2025-07-16]. Available at: https://doi.org/10.37458/ssj.2.1.7.

16. JURČÁK, V. – TREBULA, M. (2017). O vzťahu bezpečnostných a strategických štúdií. In: *Kultura Bezpieczeństwa. Nauka-Praktyka-Refleksje*, 2017, vol. 28, no. 28, pp. 94-105. ISSN 2299-4033. [online]. [cit. 2025-07-14]. DOI:10.24356/KB/28/3.

17. KAZANSKÝ, R. – CSÉFALVAY, J. (2023). Strategic Studies, Strategy, and Strategic Thinking in Study of Security. In: *National Security and the Future*, 2023, vol. 24, no. 2, pp. 7-29. ISSN 1846-1425. [online]. [cit. 2025-07-16]. Available at: https://doi.org/10.37458/nstf.24.2.1.

18. KEGLEY, C. W. (1993). The Neoidealist Moment in International Studies? Realist Myths and the New International Studies. In: *International Studies Quarterly*, 1993, vol. 37, no. 2, pp. 131-146. ISSN 0020-8833. [online]. [cit. 2025-07-16]. Available at: https://doi.org/10.2307/2600765.

19. KOLODZIEJ, E. A. (1992). Renaissance in Security Studies? Caveat Lector! In: *International Studies Quarterly*, 1992, vol. 36, no. 4, pp. 421-438. ISSN 0020-8833. [online]. [cit. 2025-07-16]. Available at: https://doi.org/10.2307/2600733.

20. KOUDELKA, Z. (2016). *Mezinárodní konflikty a bezpečnost státu*. Ostrava: Key Publishing, 2016. 74 p. ISBN 978-80-7418-264-8.

21. KÜPELI, H. (2021). Security Studies as a Subfield of International Relations: A Historical and Epistemological Perspective. In: *Turkish Journal of War Studies*, 2021, vol. 2, no. 1, pp. 38–62. ISSN 2717-7432. [online]. [cit. 2025-07-15]. Available at: https://doi.org/10.52792/tws.893428.

22. MAJCHÚT, I. (2024). Contemporary Civil-Military Relations. In: *Challenges to national defence in contemporary geopolitical situation : proceedings of the 4th International Scientific Conference*. Viľňus: Generolo Jono Žemaičio Lietuvos karo akademija, 2024, pp. 124-133 ISSN 1470-2436.

23. NEČAS, P. – PROCHÁZKA, J. (2020). *Přístupy k tvorbě bezpečnostních a obranných strategií*. Banská Bystrica: Vydavateľstvo Belianum, 2020. 202 p. ISBN 978-80-557-1656-5.

24. PARET, P. – GILBERT, F. – CRAIG, G. A. (2010). *Makers of Modern Strategy from Machiavelli to the Nuclear Age*. Princeton: Princeton University Press, 2010. 952 p. ISBN 978-1-400-83546-1.

25. PIWOWARSKI, J. – TRIFUNOVIĆ, D. – WOSZCZEK, L. (2024). Prolegomena to the scientific and practical approach to security culture in psychosocial aspects - selected issues. In: *Kultura bezpieczeństwa*, 2024, vol. 44, No. 44, pp. 144 - 163. ISSN 2299-4033. [online]. [cit. 2025-07-16]. Available at: https://kulturabezpieczenstwa.publisherspanel.com/article/549011/en.

26. ROŽŇÁK, P. – JUŘÍČEK, L. (2014). *Bezpečnostní hrozby a rizika v 21. století*. Ostrava: Key Publishing, 2014. 324 s. ISBN 978-80-7418-201-3.

27. SUCHÝ, P. (2003). Bezpečnostní a strategická studia jako součást mezinárodních vztahů. In: *Obrana a strategie*, 2003, vol. 3, č. 2, pp. 7-16. ISSN 1802-7199. [online]. [cit. 2025-07-16]. Available at: https://www.obranaastrategie.cz/filemanager/files/6370-en.pdf.

28. TVARONAVIČIENĖ, M. (2024). The Transition towards Renewable Energy: The Challenge of Sustainable Resource Management for a Circular Economy. In: *Energies*, 2024, vol. 17, no. 17, art. 4242. ISSN 1996-1073. [online]. [cit. 2025-07-14]. Available at: https://doi.org/10.3390/en17174242.

29. WALT, S. M. (1991). The Renaissance of Security Studies. In: *International Studies Quarterly*, 1991, vol. 35, no. 2, pp. 211-239. ISSN 0020-8833. [cit. 2025-07-14]. Available at: https://doi.org/10.2307/2600471.

30. ZACHAR KUCHTOVÁ, J. (2024). Umelá inteligencia a informačný chaos: Výzvy v boji proti dezinformáciám. In: *Bezpečnosť elektronickej komunikácie: zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru, 2024, s. 256-267. ISBN 978-80-8293-021-7.

ADDRESS & ©

doc. Ing. Radoslav IVANČÍK, PhD. et PhD., MBA, MSc.
Univerzita Konštantína Filozofa
Filozofická fakulta
Katedra filozofie a politológie
Hodžova 1
949 01 Nitra
Slovenská republika
rivancik@ukf.sk

DOI: 10.36682/a_2025_2_3

EU ECONOMIC SECURITY AND DUAL-USE TECHNOLOGIES IN POLITICAL, SECURITY AND RESEARCH CONTEXTS

Ekonomická bezpečnost EU a technologie dvojího využití v politickém, bezpečnostním a výzkumném kontextu

Roman HORÁK

Brno, Czech Republic

ABSTRACT: Current geopolitical developments are prompting the European Union to reassess the traditional approach in which the economy and security were perceived separately. This article therefore examines the newly introduced European Economic Security Strategy and its relationship to research and development in the field of dual-use technologies. The analysis demonstrates that the existing fragmentation of programmes and the strict separation of civil and military research are no longer sustainable. Although initiatives such as EUDIS and STEP indicate a shift, barriers in the areas of funding, innovation procurement and legislative definitions still persist. The article argues that addressing these limitations requires improved coordination among existing instruments as well as consideration of a dedicated framework for supporting dual-use research. In conclusion, the author states that effective support for dual-use technologies is crucial for enhancing the EU's economic security, strengthening its strategic autonomy and maintaining its global competitiveness.

Key words: European Union – economic security – dual-use technologies

ABSTRAKT: Současný geopolitický vývoj nutí Evropskou unii přehodnotit tradiční přístup, ve kterém se ekonomika a bezpečnost vnímaly odděleně. Tento článek proto analyzuje novou Evropskou strategii hospodářské bezpečnosti a její propojení s výzkumem a vývojem technologií s dvojím použitím. Analýza ukazuje, že dosavadní fragmentace programů a striktní oddělení civilního a vojenského výzkumu již není dále udržitelné. Přestože iniciativy jako EUDIS a STEP naznačují posun, stále přetrvávají bariéry v oblasti financování, inovačních zakázek a legislativních definic. Z uvedeného důvodu by bylo vhodné zlepšit řadu věcí, od lepší koordinace stávajících programů až po vytvoření samostatného nástroje pro duální výzkum. V závěru autor uvádí, že efektivní podpora duálních technologií je klíčová pro posílení ekonomické bezpečnosti, strategické autonomie EU a její globální konkurenceschopnosti.

Klíčová slova: Evropská unie – ekonomická bezpečnost – technologie dvojího využití

INTRODUCTION

The current development of human society is highly dynamic, volatile, unstable, and in many respects, increasingly turbulent (Ivančík, 2022). The European Union (EU) has not been

immune to these trends, and in the last decade, has increasingly faced a situation where long-standing assumptions about security, stability, and economic integration can no longer be taken for granted. The COVID-19 pandemic, Russia's aggression against Ukraine, intensifying great power rivalry, and accelerated technological transformation have exposed numerous new vulnerabilities affecting supply chains, critical infrastructure, and research and innovation ecosystems. It has become clear that the economic dimension can no longer be viewed separately from security considerations, as it has become a part of geopolitical competition in which tools such as foreign investment, technology transfer, and export restrictions are used with explicit strategic intent (Ivančík – Andrassy, 2025). In response to these challenges, the European Commission to adopt the European Economic Security Strategy, which establishes a framework for strengthening the Union's resilience and sovereignty through measures aimed at protecting key technologies, coordinating export controls, screening foreign investments, and enhancing research security, with an emphasis on balancing openness with protection (European Commission, 2023a).

At the same time, the issue of dual-use technologies, defined as technologies with potential applications in both civilian and military domains, is increasingly coming to the forefront. In an environment where the boundaries between civilian and defence sector innovations are becoming increasingly blurred, it is clear that dual-use technologies are not just a scientific and technical matter, but also a security and strategic concern. In response to this development, the European Commission published a White Paper in 2024 outlining options for enhancing support for dual-use research and development. The document identifies three basic scenarios for future action: more effective use of the existing framework, the removal of the exclusively civilian orientation in selected parts of the framework programme, and the establishment of a dedicated instrument for technologies with dual-use potential (European Commission, 2024a). The document also highlights key barriers, including the lack of a uniform definition of dual-use research, limited pathways for commercialization of research outcomes, and challenges related to aligning security requirements with existing funding and procurement mechanisms.

METHODOLOGY AND OBJECTIVE

The article aims to synthesize and critically assess European economic security policy, with particular attention to research and development of dual-use technologies. The focus is on three fundamental questions: first, which risks and tools the EU identify within the European

Economic Security Strategy and the related White Paper; second, what internal tensions emerge between research openness, competitiveness, and security requirements; and third, which politicy options and trade-offs appear realistic from the perspective of the Union’s strategic autonomy objectives and international commitments.

The article's main contribution lies in linking security-oriented analysis with the strategic implications for European R&D governance and industrial policy in the field of critical technologies. The considerations presented in the following three chapters focus on elaborating on these dimensions: first, the content and policy significance of the European Economic Security Strategy; second, the role of dual-use technologies within the European research and innovation landscape; and third, future possibilities and perspectives for the development of dual research in the context of strengthening European economic security.

From a methodological standpoint, the author uses an interdisciplinary approach, drawing primarily on methods used in security, economic, and political sciences. The relevant scientific methods employed include a combined qualitative approach consisting of scientific document analysis, content and comparative analyses, and normative policy synthesis. This method is not based on original quantitative data collection (e.g., questionnaires or statistical series), as its goal is an analytical synthesis of policies and proposals in the field of EU economic security. This approach allows for a quick and accurate capture of the nature of political decisions, their interconnections, and implications for the research and development ecosystem and industrial ecosystems with dual-use potential.

RESULTS AND DISCUSSION

European Economic Security Strategy

In 2023, the European Union unveiled its first comprehensive economic security strategy, reflecting a fundamentally changed geopolitical and technological environment. This document builds on lessons learned from the COVID-19 pandemic, Russia´s aggression against Ukraine, rising cyberattacks on public and private systems, interference with critical infrastructure, and the systematic use of economic dependencies as a tool of coercion by third countries. All these events fundamentally challenged the assumption that open trade and globalized economic exchange can be viewed as exclusively positive and stabilizing elements of the international system (European Commission, 2023a). The strategy therefore represents a significant shift in European thinking, as the economic dimension is explicitly linked to security threats and questions of political autonomy.

The strategy is structured around a three-pillar framework based on the "promote, protect, partner" logic. The first pillar emphasises the need to promote the EU's competitiveness and growth through investment in innovation, diversification of supply chains, and strengthening of the technological and industrial base. The second pillar focuses on protection against identified risks through tools such as foreign investment screening mechanisms, export controls, and measures to counter economic coercion. The third pillar highlights the importance of cooperation with a broad range of partner countries that share an interest in more resilient and secure economic relations (European Commission, 2024b). This three-pillar framework is coonceived as a dynamic structure that can respond to evolving risks while allowing for a combination of openness and selective restriction.

The strategy identified four main categories of risks. The first concerns vulnerabilities in supply chains, which became particularly evident during the COVID-19 pandemic and following Russia's disruption of energy supplies. The second category relates to the physical security and cybersecurity of critical infrastructure, including energy networks, undersea cables, and telecommunication systems. The third category involves risks associated with technological security and the leakage of knowledge, with areas such as semiconductors, quantum computing, and artificial intelligence identified as particularly sensitive. The fourth category is economic coercion, defined as the use of trade and investment measures by third countries to force Member States or European companies into political concessions (European Commission, 2023a). These risk categories share a common feature: in a globalized economy, the boundary between economics and security is increasingly blurred, and traditional tools of economic policy are acquiring strategic significance.

Key measures proposed include a revision of the foreign direct investment screening mechanism, aimed at reducing uneven application across Member States and introducing a mandatory minimum framework for all sectors considered strategic. Equally important is the expansion of monitoring capabilities for 'outbound investments'—investments by European entities in third countries in sensitive technological areas. This issue is particularly sensitive, as the EU has traditionally been an advocate for open investment flows; however, recent developments show that the absence of systematic monitoring may contribute to strengthening the capabilities of actors that could pose a threat to European security (Leichthammer, 2024). At the same time, the need to harmonise export controls is emphasised, as fragmentation of national control lists and divergent national approaches can create vulnerabilities and reduce the overall effectiveness of these measures (European Commission, 2023a).

The strategy pays special attention to research and innovation, highlighting the risk of the misuse of the openness of the academic environment and cooperation with third countries. Universities and research institutions can become targets of influence operations, or the results of joint research projects can be used for military purposes outside the EU. Therefore, the Commission proposes measures to enhance research security, i.e., to strengthen the capacity of research organisations to identify and mitigate risks arising from international cooperation. This approach is based on the principle of "as open as possible, as closed as necessary", which explicitly reflects the tension between the need to maintain openness as a driver of innovation and the obligation to protect security interests (European Commission, 2023a).

From an academic perspective, the strategy can be interpreted as a shift from the traditional model of liberalised trade and investment toward an approach that integrates security considerations into economic policymaking. This trend is not unique to the European Union. In recent years, the United States has introduced a series of measures to control semiconductor exports and restrict China´s access to advanced technologies, while China openly declares a civil-military fusion strategy. The EU thus operates in an increasingly competitive environment where technological sovereignty is acquiring a pronounced geopolitical dimension (Reiner – Stöllinger, 2025). The significance of the strategy lies in its provision of a framework for collective action among Member States and the harmonisation of measures that might otherwise remain fragmented and less effective.

Despite its ambitious scope, the strategy faces several challenges. First, there is an inherent tension between economic openness, which underpins prosperity, and the need for protection against security risks. The political debate about the scope of regulation and the degree of market intervention will therefore differ among member states, which have different economic models and ties to third countries. Second, effective implementation requires a high degree of coordination among the European Commission, Member States, and the private sector. Without this coordination, there is a risk of renewed fragmentation. Third, it remains unclear how the EU will secure sufficient resources to strengthen its technological and industrial base to reduce dependence on external actors in areas such as critical raw materials or advanced semiconductors (Calcara et al., 2025).

Overall, it can be stated that the European Economic Security Strategy represents a key step towards redefining the relationship between economics and security in the European context. Its strength lies in the clear categorisation of risks and the systematic set of tools designed to address them. Its main weakness remains the potential for fragmented implementation and the absence of a long-term vision for reconciling economic openness with

increasing security requirements. The following chapter therefore focuses on the issue of dual-use technologies, which constitute one of the most visible areas where economic and security dimensions intersect in the everyday practice of research, development, and industrial policy.

Dual-Use Technologies in the European Political and Research Context

Dual-use technologies – those with the potential to be used for both civilian and military purposes – are at the heart of the debate on European economic security. In a globalised and technologically interconnected world, the boundaries between civilian and defence research are increasingly blurred, as innovations developed in academic or commercial environments may have immediate applicability in defence systems and vice versa (Knafo, 2025). This bridging nature makes dual-use technologies a strategic priority for the EU, which recognises that maintaining a technological advantage requires systematic investment, coordination, and the reduction of existing fragmentation.

Since the beginning of the 21st century, European research and innovation framework programmes (e.g., Horizon 2020, Horizon Europe) have been designed primarily with an emphasis on civilian applications. In parallel, the European Defence Fund (EDF) was established to support projects with an explicitly military orientation (EDA, 2025). While this institutional dichotomy reflected the political sensitivity surrounding the militarisation of research, it also reinforced a structural divide between civilian and defence domains. As a result, many technological innovations remained confined within individual programmes and could not fully exploit their dual-use potential (Mueller, 2024).).

The European Commission sought to address this divide through the 2021 Action Plan on Synergies between Civil, Defence and Space Industries, which explicitly promoted "cross-fertilisation," between research and innovation activities across different sectors (European Commission, 2021). This initiative was followed by several complementary policy documents, including the European Innovation Agenda (European Commission, 2023b), the Critical Technologies for Security and Defence Roadmap (European Commission, 2022), and the European Space Strategy for Security and Defence (European Commission, 2023c). Together, these documents emphasise the need for a more coherent framework that would allow for the systematic connection between civilian and military research in areas where potential synergies are most significant, i.e., in quantum technologies, semiconductors, artificial intelligence, cybersecurity, biotechnologies, and space systems.

A concrete tool for reducing fragmentation is the European Defence Innovation Scheme (EUDIS), launched in 2022 as part of the EDF. Its goal is to create space for start-ups, SMEs, and non-defence actors who can contribute to the development of defence capabilities by leveraging technologies originally developed in civilian contexts. In 2023, the value of calls within EUDIS exceeded EUR 220 million, with strong interest in non-thematic calls focused on disruptive technologies, indicating that the business sector perceives considerable market potential in this area (European Council, 2025).

Despite these initiatives, a number of obstacles continue to limit the effective exploitation of the potential of dual-use technologies (Sun, 2024). The first is the absence of a uniform definition of "dual use" within the European research and innovation framework. Although EU export control legislation provides a clear classification of dual-use items, support mechanisms in the R&D field remains ambiguous, complicating cooperation between institutions such as the European Investment Bank and the European Commission (Béraud-Sudreau et al., 2023). Another barrier is the limited ability to translate research outcomes into commercial or defence applications. Many projects remain at the pilot stage because there is insufficient innovative procurement and the absence of an initial customer capable of supporting large-scale deployment. This phenomenon is often referred to as the "European Innovation Gap" (Veugelers, 2022).

Another problem arise from the differing cultures and logic of funding between civilian and defence research. Horizon Europe prioritises scientific excellence, open cooperation, and the dissemination of results, whereas the EDF operates under stricter security requirements, involves classified information, and limits participation to a narrower group of eligible entities. These differences create barriers that complicate synergies and reduce attractiveness for entities operating on the border between the two worlds. An example is the limited participation of the defence sector in European Innovation Council (EIC) schemes, where access for projects with a military focus is practically excluded (Cutts, 2025).

At the same time, the potential of dual-use research is enormous. Many critical technologies originate primarily in the civilian sector, where there are higher levels of investment, shorter innovation cycles, and lower development costs. Technologies such as drones, satellite services, cyber infrastructure, and artificial intelligence applications are examples of areas where the transfer of technologies from the civilian to the military environment is already shaping modern military doctrine today. Conversely, some defence technologies, funded through the EDF, can find civilian applications in infrastructure security, emergency services, or crisis management. This bidirectional transfer represents an important

source of added value that can strengthen European competitiveness and contribute to strategic autonomy (Guntrum et al., 2023).

In this context, the Strategic Technologies for Europe Platform (STEP), adopted in 2023, has a special role in this area. STEP aims to support Europe's technological lead in critical technologies with high dual-use potential, including quantum computing, biotechnologies and zero-emission industrial processes. Its goal is to align investments and facilitate the combined use of multiple European funding instruments, including cohesion policy funds and InvestEU (European Union, 2023). As such, STEP provides a framework where economic security, industrial policy, and technological sovereignty intersect.

Despite these efforts, the European approach to dual-use technologies remains fragmented, which limits its overall effectiveness. The long-standing political separation between civilian and military research was historically justified, but undercurrent geopolitical context, it increasingly appears unsustainable. Ongoing debates on redefining framework programmes, strengthening integration, and supporting dual research is therefore a fundamental element of the broader discussion about the European Union's strategic autonomy.

FUTURE POSSIBILITIES AND PROSPECTS FOR SUPPORTING DUAL-POTENTIAL R&D

The future of European support for dual-use research and development is closely linked to the search for a balance between openness and security, as well as between economic competitiveness and political autonomy. The 2024 European Commission White Paper outlines three scenarios for the future direction of policy in this area, each associated with specific advantages and risks (European Commission, 2024a). These scenarios reflect the growing tension between the need to better integrate civilian and military research and the long-standing tradition of their strict separation.

The first scenario focuses on strengthening the use of existing frameworks, especially Horizon Europe, the European Defence Fund, and related instruments, through improved coordination and interconnection. This option is the least politically controversial, as it does not require fundamental changes to the legal basis or a major restructuring of existing programmes. It allows for a gradual improvement of synergies while avoiding potential conflicts with member states that prefer to maintain a clear distinction between civilian and military research. The risk of this scenario, however, is that it may fall short of expectations in terms of

breakthrough innovation and fail to eliminate the structural barriers that have so far limited deeper integration.

The second scenario involves removing the exclusively civilian focus in selected parts of Horizon Europe and enabling the funding of projects with explicit dual-use potential. This approach would open doors for start-ups and SMEs that operate at the interface between civilian and military applications and would allow for more flexible technology transfer. It could also reduce the innovation gap between Europe and global competitors, such as the United States and China, where civil–military integration has long been practised. This scenario is politically sensitive, as it challenges the traditional civilian orientation of European framework programmes and may encounter resistance from parts of the academic community that emphasise openness and the independence of research.

The third scenario proposes the creation of a separate instrument to support the research and development of dual-use technologies. Such an instrument could function as a 'bridge' between Horizon Europe and the EDF, targeting projects that combine civilian and military applications. This approach would allow for targeted funding of key technologies, including artificial intelligence, quantum computing, biotechnologies, and space applications, while also providing a clear political identity for a European dual-use programme. The weakness is the need for additional financial resources at a time when the EU budget is already under significant pressure from competing priorities, ranging from climate policy to social cohesion (European Commission, 2022b, 2025a, 2025b).

All three scenarios share a common starting point: the recognition that the status quo is unsustainable and that it is necessary to create a framework that will reduce fragmentation, strengthen synergies, and improve the transfer of research results into practical applications. The debate therefore concerns the appropriate level of ambition and political feasibility. Some member states, particularly those with an advanced defence industry, favour more radical scenarios, while others advocate a more cautious approach aimed at avoiding political polarisation.

The question of supporting dual-use research and development is closely linked to the broader concept of European strategic autonomy, particularly the EU’s ability to develop key technological capacities independently of external suppliers. In the context of the war in Ukraine and the growing geopolitical rivalry between the USA and China, it is clear that European dependence on third countries for semiconductors, batteries, and critical raw materials represents not only an economic vulnerability but also a security risk (Umbach, 2024).

Therefore, strengthening dual-use research and development is seen as one of the tools to mitigate this dependence and strengthen the European technological base.

The international dimension further underlines this challenge. The United States has long supported a model of civil-military integration through programmes such as the Defense Advanced Research Projects Agency (DARPA), the Small Business Innovation Research (SBIR) scheme, and close cooperation between the Department of Defense and Silicon Valley technology giants. China, on the other hand, openly promotes a 'civil-military fusion' strategy, which integrates all segments of the economy into the building of military capabilities. The EU, which has traditionally stressed the civilian nature of research, faces a strategic dilemma: maintaining a rigid separation risks technological lag, while deeper integration requires solutions compatible with European values and legal constraints (Rousseaux, 2024).

Investment and innovative procurement will be a key factor in shaping future outcomes. Without European public authorities acting as first customers, a substantial share of research outputs is likely to remain at the prototype stage. Therefore, the European Commission emphasises the need to stimulate demand for innovative solutions from the public sector and to create mechanisms that enable start-ups and SMEs to enter the market more effectively. This approach also reduces the risk of technological leakage by strengtheniing links between research institutions, industry, and public authorities within the EU (European Commission, 2025c; Radic – Auer, 2025).

The future direction of European support for dual-use research cannot therefore be viewed merely as a technical question about the setup of programmes, but as a strategic decision with long-term geopolitical implications. The outcome of the discussion about which scenario will be adopted will determine whether the EU will succeed in overcoming existing fragmentation and building a robust and competitive ecosystem capable of facing global competition (Rekowski, 2025). In this sense, it can be said that the issue of dual-use research is one of the key tests of European strategic autonomy.

CONCLUSION

The European Union is entering a period where the boundary between economics and security is becoming increasingly unrecognisable. The 2023 Economic Security Strategy confirms that traditional assumptions based on free trade and globalisation are no longer sufficient to address current threats. The identified risk categories – from vulnerabilities in supply chains and threats to critical infrastructure to economic coercion – show that the

European economy has become both a target and a tool of geopolitical competition. In this context, economic security can no longer be understood as a secondary concern, but rather as a fundamental pillar of the Union's resilience and sovereignty.

The analysis of dual-use technologies has shown that this is an area where economic, technological, and security dimensions intersect most directly. The European approach, historically based on a strict separation between civilian and military research, while reflecting value-based and political priorities, is proving to be a constraint in the current geopolitical environment. Programme fragmentation, the absence of a uniform definition of dual use, and the limited capacity to translate research outputs into practice reduce the overall effectiveness of the European innovation ecosystem. Instruments such as EUDIS and STEP represent important steps in the right direction, but so far, they have not been able to overcome the basic structural barriers.

The discussion about future possibilities, presented in the 2024 White Paper, clearly shows that the status quo is unsustainable. The proposed scenarios, ranging from a slight improvement of existing frameworks to the creation of a new instrument for dual-use technologies, reflect a persistent tension between political feasibility and the level of ambition. From the perspective of economic security, it is crucial for Europe to succeed in eliminating fragmentation and establishing a functional link between civilian and defence research. Only under these conditions can critical technologies – from semiconductors to artificial intelligence – be developed and used in a way that serves European strategic interests and limits dependence on external actors.

The analysis therefore confirms that economic security and dual-use research are inseparably interconnected. Economic security provides the policy and regulatory framework aimed at protecting critical technologies and reducing strategic dependencies, while dual-use research is the practical mechanism that enables the development of these technologies. The effectiveness of one dimension is thus directly dependent on the effectiveness of the other. Without an effective system for supporting dual-use research, economic security risks losing a substantial part of its practical relevance; conversely, without an effective economic security strategy, dual-use research remains exposed to risks such as technological leakage or economic coercion.

Looking ahead, European economic security will increasingly depend on the Union’s ability to preserve technological capabilities and independence in critical sectors. Strengthening investment in research and innovative procurement, deepening synergies between civilian and defence sectors and systematically involving the private sector will be decisive factors for

success. At the same time, it will be necessary to develop partnerships with democratic allies so that the EU can face global competition from actors such as the United States and China, which already operate integrated models of civil-military research.

If the EU succeeds in addressing these challenges, it can become an actor that not only protects its economic and security interests but also contributes to the creation of a more stable and secure international environment. Economic security would then cease to be merely a reactive response to crises and instead become a constitutive element of European strategic autonomy with broader global relevance.

LITERATURE AND INFORMATION SOURCES USED

1. CALCARA, A. – TEER, J. – ZACCAGNINI, I. (2025). Technological underpinnings of European autonomy and US-China competition. In: *Journal of European Integration*, 2025, Vol. 47, No. 6, pp. 943-963. ISSN 1477-228. DOI: 10.1080/07036337.2025.2536828.
2. CUTTS, E. (2025). Europe mulls boosting military R&D with civilian science funding. In: *Science*, 2025. Available at: https://www.science.org/content/article/europe-mulls-boosting-military-r-d-civilian-science-funding.
3. EDA. (2025). The European Defence Fund (EDF). In: *European Defence Agency*, 2025. Available at: https://eda.europa.eu/what-we-do/EU-defence-initiatives/european-defence-fund-(edf).
4. EUROPEAN COMMISSION. (2023a). *European Economic Security Strategy*. In: *European Commission*, 2023. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN%3A2023%3A20%3AFIN.
5. EUROPEAN COMMISSION. (2024a). White Paper on options for enhancing support for R&D involving technologies with dual-use potential. In: *European Commission*, 2024. Available at: https://research-and-innovation.ec.europa.eu/document/download/7ae11ca9-9ff5-4d0f-a097-86a719ed6892_en?filename=ec_rtd_white-paper-dual-use-potential.pdf.
6. EUROPEAN COMMISSION. (2024b). Advancing European economic security: an introduction to five new initiatives. In: *European Commission*, 2024. Available at: https://commission.europa.eu/system/files/2024-01/Communication%20on%20European%20economic%20security.pdf.
7. EUROPEAN COMMISSION. (2021). Action Plan on synergies between civil, defence and space industries. In: *European Commission*, 2023. Available at: https://commission.europa.eu/system/files/2021-03/action_plan_on_synergies_en_1.pdf.
8. EUROPEAN COMMISSION. (2022a). Roadmap on critical technologies for security and defence. In: *European Commission*, 2022. Available at: https://commission.europa.eu/system/files/2022-02/com_2022_61_1_en_act_roadmap_security_and_defence.pdf.

9. EUROPEAN COMMISSION. (2022b). Joint Communication on the Defence Investment Gaps Analysis and Way Forward. In: *European Commission*, 2022. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022JC0024.
10. EUROPEAN COMMISSION. (2023b). The New European Innovation Agenda. In: *European Commission*, 2023. Available at: https://research-and-innovation.ec.europa.eu/strategy/support-policy-making/shaping-eu-research-and-innovation-policy/new-european-innovation-agenda_en.
11. EUROPEAN COMMISSION. (2023c). European Space Strategy for Security and Defence. In: *European Commission*, 2023. Available at: https://defence-industry-space.ec.europa.eu/eu-space/eu-space-strategy-security-and-defence_en.
12. EUROPEAN COMMISSION. (2025a). Interim Evaluation of the Horizon Europe Framework Programme for Research and Innovation (2021 - 2024). In: *European Commission*, 2025. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025SC0110.
13. EUROPEAN COMMISSION. (2025b). Commission Implementing Decission on on the financing of the European Defence Fund and the adoption of the work programme for 2025. In: *European Commission*, 2025. Available at: https://defence-industry-space.ec.europa.eu/document/download/ffa3769f-3b6d-4b07-b3d4-a5c156a5fde3_en?filename=EDF%20Work%20Programme%202025%20Part%20II.pdf.
14. EUROPEAN COMMISSION. (2025c). The EU Startup and Scaleup Strategy. In: European Commission, 2022. Available at: https://research-and-innovation.ec.europa.eu/document/download/8f899486-6e4e-48df-8633-9582375f41eb_en.
15. EUROPEAN COUNCIL. (2025). Accompanying the document Interim evaluation of the European Defence Fund. In: *European Council*, 2025. Available at: https://data.consilium.europa.eu/doc/document/ST-11026-2025-ADD-1/en/pdf.
16. EUROPEAN UNION. (2022). EU Defence Innovation Scheme (EUDIS). In: *European Union*, 2022. Available at: https://eudis.europa.eu/index_en.
17. EUROPEAN UNION. (2023). Strategic Technologies for Europe Platform. In: *European Union*, 2023. Available at: https://strategic-technologies.europa.eu/index_en.
18. GUNTRUM, L. G. – SCHWARTZ, S. – REUTER, C. (2023). Dual-Use Technologies in the Context of Autonomous Driving: An Empirical Case Study from Germany. In: *Zeitschrift für Außen – und Sicherheitspolitik*, 2023, Vol. 16, pp. 53-77. ISSN 1866-2196. DOI: 10.1007/s12399-022-00935-3.
19. IVANČÍK, R. – ANDRASSY, A. (2025). Discussing EU's Security Identity: Defence Spending, Strategic Autonomy and Transition from Normative Ambition to Geopolitical Reality. In: *Entrepreneurship and Sustainability Issues*, 2025, Vol. 13, no. 1, p. 411-425. ISSN 2345-0282. DOI: 10.9770/c2892383535.
20. IVANČÍK, R. (2022). On European Union Partnership and Cooperation in the Field of Security and Defence. In: *Auspicia*, 2022, Vol. 19, No. 2, pp. 65-75. ISSN 2464-7217. DOI: 10.36682/a_2022_2_7.

21. KNAFO, S. (2025). Report on European technological sovereignty and digital infrastructure. In: *European Parliament*, 2025. Available at: https://www.europarl.europa.eu/doceo/document/A-10-2025-0107_EN.html.
22. LEICHTHAMMER, A. (2024). Navigating the Geoeconomic Tide: The Commission's quest for a policy compass. In: *Jacques Delors Centre & Hertie School*, 2024. Available at: https://www.delorscentre.eu/en/publications/detail/publication/navigating-the-geoeconomic-tide.
23. MUELLER, T. (2024). Strategic options for the European defence industry in the 2020s. In: *Defense & Security Analysis*, 2024, Vol. 41, No. 1, pp. 49-80. ISSN 1475-1801. DOI: 10.1080/14751798.2024.2418163.
24. RADIC, L. – AUER, D. (2025). A Europe Fit for the Age of Startups. In: *International Center for Law & Economics*, 2025. Available at: https://laweconcenter.org/resources/a-europe-fit-for-the-age-of-startups-rhetoric-and-reality-in-the-eus-digital-package.
25. REINER, C. – STÖLLINGER, R. (2025). Europe's Quest for Technological Sovereignty: A Feasible Path Amidst Global Rivalries. In: *Social Europe*, 2025. Available at: https://www.socialeurope.eu/europes-quest-for-technological-sovereignty-a-feasible-path-amidst-global-rivalries.
26. REKOWSKI, M. (2025). Building Strategic Autonomy in the European Union. In: *Studia Europejskie – Studies in European Affairs*, 2025, Vol. 29, No. 1, pp. 249-271. ISSN 2719-3780. DOI: 10.33067/SE.1.2025.13.
27. SUN, K. (2024). Hidden Hurdles | The Untold Challenges of Shipping Dual-Use Technology. In: *TecEx*, 2024. Available at: https://tecex.com/the-untold-challenges-of-shipping-dual-usetechnology.
28. UMBACH, F. (2024). Securing Europe's Independence in Critical Raw Materials and Technological Components. In: *FocusFuture*, 2024. Available at: https://www.martenscentre.eu/wp-content/uploads/2024/12/Securing-Europes-Independence-in-Critical-Raw-Materials-and-Technological-Components.pdf.
29. VEUGELERS, R. (2022). The European Union's growing innovation divide. In: *Bruegel*, 2022. Available at: https://www.bruegel.org/policy-brief/european-unions-growing-innovation-divide.

ADDRESS & ©

doc. Ing. Roman HORÁK, CSc.
Univerzita obrany
Fakulta vojenského leadershipu
Katedra řízení zdrojů
Kounicova 65, 662 10 Brno
Czech Republic
roman.horak@unob.cz

BEZPEČNOST • SAFETY

DOI: 10.36682/a_2025_2_4

THE ECONOMIC CONSEQUENCES OF THE RUSSIAN INVASION OF UKRAINE: IMPACT ON THE ENERGY SECURITY AND PRICE STABILITY OF THE SLOVAK REPUBLIC

Ekonomické dôsledky ruskej invázie na Ukrajinu: vplyv na energetickú bezpečnosť a cenovú stabilitu Slovenskej republiky

Simona KOVÁČOVÁ – Martin JARABÁK

Sládkovičovo, Slovak Republic

ABSTRACT: The Russian invasion of Ukraine in 2022 significantly altered the economic landscape of the European Union, with particularly profound consequences for the Slovak Republic. This paper focuses on the economic aspects of the crisis, specifically its effects on the energy sector, rising energy prices, inflation, and Slovakia's energy dependence on Russia. The analysis is based on data from Eurostat, the Statistical Office of the Slovak Republic, and relevant academic literature. It presents concrete data on energy imports, the decline in gas consumption, and the development of electricity and gas prices for both households and industry. The paper highlights the challenges associated with the energy transition and emphasizes the need to enhance resilience against external shocks.

Key words: Russian invasion of Ukraine – Slovak Republic – energy security – inflation – public policy response

ABSTRAKT: Ruská invázia na Ukrajinu v roku 2022 výrazne zmenila ekonomickú situáciu v Európskej únii, pričom mimoriadne závažné dôsledky mala pre Slovenskú republiku. Príspevok sa zameriava na ekonomické aspekty krízy, konkrétne na vplyv na energetický sektor, rast cien energií, infláciu a energetickú závislosť Slovenska od Ruska. Analýza je založená na údajoch z Eurostatu, Štatistického úradu Slovenskej republiky a relevantných akademických štúdií. Príspevok uvádza konkrétne údaje týkajúce sa dovozu energií, poklesu spotreby plynu a vývoja cien elektriny a plynu pre domácnosti aj priemysel. Štúdia zároveň poukazuje na výzvy energetickej transformácie a potrebu posilnenia odolnosti voči vonkajším šokom.

*Kľúčové slová***:** ruská invázia na Ukrajinu – Slovenská republika – energetická bezpečnosť – inflácia – reakcia verejnej politiky

INTRODUCTION

Energy security and price stability are fundamental prerequisites for the economic and social stability of any state. The military aggression of the Russian Federation against Ukraine,

which began in February 2022, had not only security and geopolitical consequences but also a significant economic dimension. It severely disrupted the functioning of the European energy market, led to a sharp increase in energy prices, and consequently contributed to a surge in inflation affecting the entire European Union. The Slovak Republic, as a country with a high level of dependence on energy imports from Russia, found itself in a particularly vulnerable position, especially with regard to the supply of natural gas, oil, and nuclear fuel.

In response to the emerging crisis, a range of measures was adopted to diversify supply chains and reduce energy dependency. However, these changes were accompanied by substantial economic costs that impacted the business sector, public finances, and the daily lives of citizens. The rapid increase in energy prices was reflected in consumer prices, business costs, and, subsequently resulted in a significant rise in the inflation rate.

The aim of this paper is to analyze the economic consequences of the Russia–Ukraine conflict, with a focus on the development of Slovakia's energy dependency, changes in energy prices, and the inflation trajectory during the period 2022–2023. The article also highlights the degree of success of diversification measures and examines the effectiveness of policies aimed at mitigating the impact of the crisis on the Slovak economy and population. The analysis is based on official statistical data, scholarly literature, and data from international institutions, with the primary objective of providing an expert reflection on the economic aspects of this crisis period in the context of the Slovak economy.

METHODOLOGY AND OBJECTIVE

The examination of the economic impacts of armed conflict requires contextualization within a broader framework of economic theory. Wars represent external shocks that disrupt market stability and have far-reaching effects on production, consumption, price levels, and economic growth. From a theoretical standpoint, it is appropriate to approach this issue through a combination of supply-shock theory, commodity dependency theory, and macroeconomic models of inflation. According to the classical AS-AD (aggregate supply – aggregate demand) model, an external supply shock, such as an interruption in energy supplies, shifts the aggregate supply curve to the left, resulting in higher prices and a decrease in real GDP (Blanchard, 2017).

The theory of energy security emphasizes the risks associated with unilateral dependence on energy imports, which is particularly relevant in the case of Slovakia. Prior to 2022, the country relied predominantly on imports of natural gas, oil, and nuclear fuel from the Russian Federation. As Yergin (2006) states, the diversification of energy sources is a key

condition for maintaining national security and economic stability. Energy dependence creates asymmetric power relationships that can be exploited during times of conflict.

Macroeconomic theory offers several approaches to explaining rising price levels. In 2022-2023, inflation in Slovakia was primarily cost-push in nature, driven by increases in energy and input prices. According to the Keynesian concept, such inflation results from higher production costs being passed on to final consumers, manifesting as an increase in the Consumer Price Index (CPI) (Samuelson & Nordhaus, 2010). Rising prices for gas and electricity also generate secondary effects in the form of more expensive food and services, thereby reducing the real purchasing power of the population.

Methodologically, this paper is based on a descriptive analysis of statistical data from both domestic and international sources, particularly Eurostat, the Statistical Office of the Slovak Republic, Enerdata, Macrotrends, and European Commission reports. A comparative approach is also employed to examine developments in key economic indicators (e.g., inflation, energy prices, and gas consumption) before and after the outbreak of the conflict. Secondary analysis of scientific studies and think-tank reports (e.g., Bruegel, IEA) serves to interpret the observed phenomena within a broader European context and to formulate conclusions with practical relevance for public policy.

This framework forms the basis for further analysis of the impacts of the Russia–Ukraine conflict on the Slovak economy in terms of energy dependence, price stability, and economic resilience. In this way, economic theory provides the analytical tools necessary to understand the mechanisms that have shaped economic reality under crisis conditions.

SLOVAKIA'S ENERGY DEPENDENCE AND ITS IMPACTS DURING THE CRISIS

Energy dependence represents a significant economic and geopolitical factor that determines a country's resilience to external shocks. The Slovak Republic has long been among the countries with a high degree of dependence on energy imports from the Russian Federation. Prior to the outbreak of the war in Ukraine in 2022, more than 85% of Slovakia's natural gas, oil, and nuclear fuel originated from Russia. This dependence resulted from long-term contracts, historical infrastructure ties, and the cost advantages of Russian energy supplies.

According to data from the Statistical Office of the Slovak Republic and Eurostat, in 2021, natural gas imports from Russia accounted for approximately 26% of Slovakia's total energy consumption. The supply of nuclear fuel (23%) and oil (21%) was also heavily dependent on Russian sources. In total, more than two-thirds of the Slovak Republic's energy

balance relied on imports from a single country, representing a significant security and economic risk (Statistical Office of the Slovak Republic, 2021).

The energy balance of Slovakia in 2021 was as follows:

Commodity	Volume (in million EUR)	Share of Total Consumption
Natural gas	4,551.1	26%
Nuclear fuel	4,051.1	23%
Oil and petroleum products	3,714.4	21%
Solid fossil fuels	2,823.3	16%
Renewables and other sources	2,325.1	13%
Non-renewable waste	273	1%

Source: *Statistical Office of the Slovak Republic, Eurostat (2021).*

The high concentration of energy supply from a single source became a critical issue following the outbreak of the war. The threat of supply disruptions and geopolitical coercion created an urgent need for diversification. Slovakia began signing contracts with alternative suppliers of gas and electricity, including companies such as ENI, RWE, SNAM, and Enel. The Slovak Gas Industry (SPP) also secured LNG deliveries from Norway and non-EU countries.

Despite these efforts, the level of dependence remained high. By the end of 2022, according to data from expert studies, as much as 60% of Slovakia's gas supply was still sourced from the Russian Federation (Puntíková et al., 2023). This indicates the limited capacity for rapid transformation of the country's energy mix. Moreover, the higher prices of alternative supplies led to increased energy costs, which were subsequently reflected in consumer prices and contributed to elevated inflation levels (Puntíková et al., 2023).

The economic consequences of high energy dependence can be divided into direct and indirect effects. Direct effects include rising commodity prices, supply uncertainty, increased costs related to alternative transit routes, and the need to invest in new infrastructure. Indirect impacts involve pressure on public finances, deterioration of the business environment, and reduced competitiveness of Slovak industry. Furthermore, households faced rising energy bills, which led to the introduction of state compensation measures and price regulation.

In conclusion, due to long-neglected energy vulnerabilities, Slovakia found itself in a situation that required strategic decisions to be made within a short timeframe and under significant economic pressure. The experience of the years 2022-2023 underscores the necessity of systematically reducing energy dependence, developing domestic energy production, and increasing energy efficiency as long-term objectives of economic policy.

THE RISE IN ENERGY PRICES AND THEIR IMPACT ON INFLATION AND THE ECONOMY

The war in Ukraine led to an unprecedented increase in energy prices across Europe, with Slovakia among the countries that experienced significant cost increases for both households and industry. According to Eurostat (2023), electricity prices for households in the EU rose by an average of 32% between the second half of 2021 and the second half of 2022. In Slovakia, the increase amounted to 18%, the second-lowest in the EU after Croatia, largely due to extensive price regulation and state subsidies (Eurostat, 2023).

A similar trend can be observed in the development of gas prices for households during the same period. While the average increase across the EU reached 75%, gas prices for Slovak households rose by only 18% (Eurostat, 2023). Despite the relatively low percentage increase, Slovak households paid the lowest absolute gas price in the EU, averaging €4.5 per 100 kWh in the second half of 2022.

In the industrial sector, the increase in costs was even more pronounced. Gas prices for industrial enterprises rose year-on-year by as much as 90% in some months of 2022, while electricity prices peaked in the second half of the same year (Eurostat, 2023). Although prices stabilized somewhat in 2023, they remained significantly elevated compared to the pre-crisis period. The average electricity price for households in the EU in the first half of 2023 was 23.2 euro cents per kWh, whereas in Slovakia it stood at 17.1 euro cents per kWh (Eurostat, 2023).

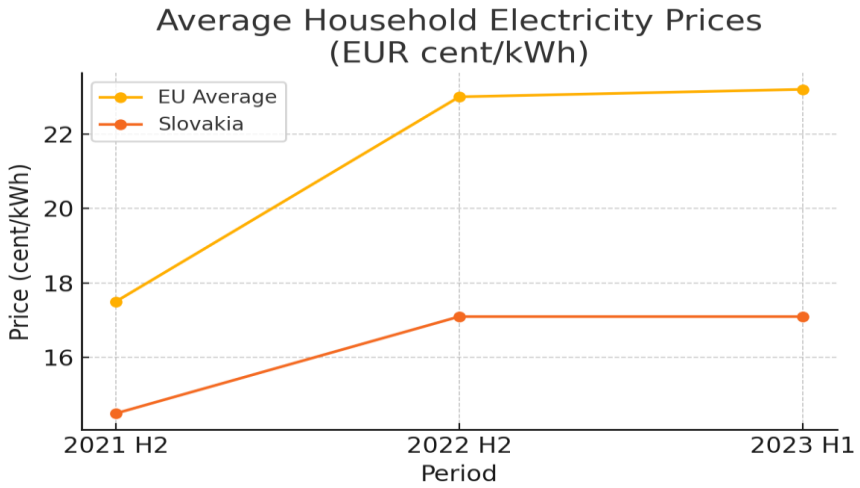
The surge in energy prices directly translated into inflationary pressures. In 2022, the average inflation rate in Slovakia reached 12.8%, with energy-related categories, such as housing, water, electricity, gas, and other fuels, recoding year-on-year price increases exceeding 20% (Statistical Office of the Slovak Republic, 2023). These figures are consistent with the cost-push inflation model, where overall price levels rise due to external inputs and supply-side shocks (Samuelson & Nordhaus, 2010).

Higher energy costs increased the overall operating expenses of businesses, significantly impacting energy-intensive sectors such as chemicals, metallurgy, and building materials production. Many companies were forced to halt production or to substantially raise product prices, further intensifying inflationary pressures. These secondary effects also impacted consumers and had a pronounced impact on real wages, which declined by 4.5% in 2022 (Statistical Office of the Slovak Republic, 2023).

Although the government implemented several measures to mitigate the effects of the energy price shock, including caps on household energy prices and subsidies for businesses, the impact of these interventions was only partial. Public expenditure on compensation measures

reached nearly 2% of GDP in 2022 (Ministry of Finance of the Slovak Republic, 2023), placing additional strain on public finances. From a macroeconomic perspective, the energy price crisis deepened existing structural weaknesses in the economy and revealed a limited level of preparedness for external shocks.

Figure 1: Average Household Electricity Prices in Slovakia and EU (EUR cent/kWh)



Source: Eurostat (2021–2023).

POLITICAL RESPONSES, ENERGY CONSUMPTION AND ECONOMIC RESILIENCE

The unprecedented energy crisis triggered by the war in Ukraine forced governments across the European Union to adopt urgent policy measures aimed at mitigating the socio-economic consequences of rising energy prices. Slovakia, as one of the most affected countries due to its high dependence on Russian gas and oil, implemented a combination of fiscal and regulatory interventions. These measures included price caps for households, compensation schemes for vulnerable groups, and direct subsidies for energy-intensive industries. In 2022, the Slovak government allocated over €1.5 billion to support energy affordability and stabilize inflationary pressures (Ministry of Finance SR, 2023). (IMF, 2023; OECD, 2023).

Despite these interventions, Slovakia recorded only a marginal reduction in natural gas consumption. According to Eurostat (2023b), natural gas consumption in the EU decreased by 19.3% between August 2022 and January 2023 compared to the average for the same months in 2017–2022. By contrast, Slovakia managed to reduce its gas consumption by only 1%, making it one of the least responsive countries in terms of energy savings. This outcome indicates structural rigidity in energy demand and limited flexibility in switching to alternative energy sources. (Eurostat, 2023b; IEA, 2023).

The limited decline in consumption can be attributed to several factors. First, a significant share of natural gas consumption is related to residential heating, where substitution options are limited in the short term. Second, many industrial processes in Slovakia are gas-dependent, and their operation is closely linked to the country's export-oriented economic structure. Third, the relatively mild winter of 2022/2023 reduced incentives for more pronounced behavioural changes in households (Bruegel, 2022).

From a macroeconomic perspective, the resilience of the Slovak economy during the energy crisis was partially supported by temporary government interventions but remained vulnerable to external shocks. While these interventions were effective in preventing immediate socio-economic destabilization, they imposed a significant burden on public finances. As the crisis persisted, concerns about fiscal sustainability and inflation expectations became more pronounced.

In conclusion, Slovakia’s political response helped to cushion the short-term impact of the energy crisis. However, the relatively low level of consumption adjustment, combined with high fiscal costs, highlights the need for more structural and long-term solutions. These include investments in energy efficiency, the development of renewable energy sources, and greater diversification of energy suppliers to enhance long-term economic resilience.

Moreover, the crisis revealed deeper structural vulnerabilities in Slovakia’s energy governance framework. The lack of timely diversification policies prior to 2022, insufficient investment in renewable energy infrastructure, and underdeveloped energy storage capacities contributed to limited systemic preparedness. The lessons drawn from the crisis underline the importance of coordinated EU-level action in energy solidarity, cross-border infrastructure development, and the strengthening of a unified energy market that enhances the resilience of small and import-dependent economies such as Slovakia (European Commission, 2023; Energy Community, 2022).

ECONOMIC OUTLOOK AND LONG-TERM POLICY IMPLICATIONS

The energy crisis triggered by the Russian invasion of Ukraine not only caused short-term disruptions but also exposed fundamental structural challenges in Slovakia’s economic model. As a small open economy with a high degree of energy import dependence, Slovakia faces considerable risks to both industrial competitiveness and fiscal sustainability. The long-term economic outlook is therefore closely linked to the country´s ability to adapt to new geopolitical and market conditions.

According to the forecasts by the National Bank of Slovakia (NBS, 2023), moderate economic growth expected in the coming years, with GDP growth projected at 1.7% in 2024 and 2.5% in 2025. However, these projections are subject to substantial uncertainty. Energy prices remain volatile, external demand is fragile, and inflationary pressures persist despite central bank interventions. The European Central Bank (ECB, 2023) notes that core inflation across the euro area is expected to remain above the 2% target throughout 2024, further complicating monetary policy coordination and constraining real wage growth.

From a structural perspective, Slovakia must accelerate the diversification of its energy mix. The International Energy Agency (IEA, 2023) emphasizes that sustained investment in renewable energy sources and energy storage systems is essential to ensure long-term energy security. Although Slovakia has made some progress, particularly in solar and hydro power, the share of renewables in total final energy consumption remains below the EU average. This discrepancy poses risks not only in terms of resilience but also in fulfilling EU climate obligations under the Fit for 55 package and the European Green Deal.

Another critical challenge lies in improving energy efficiency, particularly in the industrial and building sectors. The OECD (2023) highlights that targeted investments in insulation, heating systems, and energy management technologies can significantly reduce energy demand and enhance economic resilience. In this context, public policy must shift from compensatory subsidies towards proactive structural reforms, supported by EU funding instruments and green finance mechanisms.

Fiscal implications of the energy crisis are also significant. The Ministry of Finance of the Slovak Republic (2023) warns of rising budget deficits if temporary compensatory measures become permanent. Without a medium-term fiscal consolidation strategy, the long-term debt trajectory may become unsustainable. This risk is particularly relevant as the government seeks to invest heavily in energy infrastructure while maintaining social protection mechanisms.

Strategic foresight must therefore include the development of national capacities in energy technology innovation, workforce upskilling and regional cooperation. Slovakia's participation in regional energy platforms, such as the Three Seas Initiative or enhanced cooperation within the V4 framework, can support diversification of energy routes and strengthen geopolitical stability.

In conclusion, the energy crisis represents a turning point for Slovakia’s economic policy. Short-term stabilization must be complemented by long-term adaptation strategies that enhance energy independence, accelerate decarbonization, and strengthen macroeconomic

resilience. The effectiveness of these measures will determine Slovakia's ability to withstand future shocks and maintain competitiveness in an increasingly fragmented global economy.

To fully understand the long-term economic trajectory of Slovakia in the post-crisis environment, it is necessary to move beyond short-term macroeconomic projections and focus on structural vulnerabilities, global market dynamics, and domestic policy capacity. One of the most pronounced vulnerabilities remains the country's heavy industrial structure, particularly its dependence on the automotive sector. This sector, while highly productive, is both energy-intensive and export-dependent. Any prolonged increase in energy costs or disruptions in global supply chains could significantly undermine Slovakia's competitive position (World Bank, 2023).

Furthermore, the crisis exposed weaknesses in the governance and regulatory frameworks governing energy and environmental policy. According to the Energy Policy Review of Slovakia by the International Energy Agency (IEA, 2022), institutional coordination remains fragmented, with overlapping competencies among ministries and limited implementation capacity at the regional and municipal levels. A more integrated approach to energy transition governance is therefore critical to ensure coherence, efficiency, and accountability.

Labor market implications also deserve close attention. As Slovakia moves towards a more sustainable and low-carbon economy, reskilling and upskilling of the workforce will be required. The OECD Skills Outlook (2023) warns of potential labor displacement in carbon-intensive industries if adequate training and support mechanisms are not established. Strategic investment in education, vocational training, and innovation ecosystems will be essential to enable the workforce to adapt to emerging sectors.

At the regional level, disparities between western and eastern Slovakia may deepen in the absence of targeted interventions. Regions characterized by lower economic diversification and higher levels of energy poverty face an increased risk of stagnation. EU cohesion funds and the Just Transition Mechanism should be leveraged to address spatial inequalities and promote inclusive development (European Commission, 2023b).

Moreover, the international dimension of Slovakia's economic outlook must be taken into account. As a member of the euro area and the EU internal market, Slovakia's recovery and structural transformation are embedded within broader European strategies. Participation in joint energy procurement schemes, regional interconnectivity initiatives, and coordinated climate policy will determine the country's strategic positioning within the evolving European energy architecture (European Council, 2023).

Finally, strengthening institutional resilience, policy coherence, and strategic foresight capacities should become central pillars of Slovakia's post-crisis governance framework. This requires not only technical reforms but also fostering public trust, improving communication of policy objectives, and ensuring transparent use of recovery and resilience resources. The European Court of Auditors (2023) emphasizes that effective absorption of EU funds remains a persistent challenge in Slovakia, which could hamper implementation of necessary structural reforms.

CONCLUSION

The economic implications of the war in Ukraine and the ensuing energy crisis have severely tested Slovakia's economic, institutional, and strategic capacities. The country's high dependence on imported fossil fuels, particularly from the Russian Federation, exposed it to acute vulnerabilities that translated into price shocks, fiscal pressures, and constrained policy options. Although short-term government interventions helped to mitigate the immediate social impact of rising energy prices, they also revealed deeper structural shortcomings in energy diversification, governance capacity, and long-term resilience planning.

The analysis of economic indicators, government policies, and comparative data from other EU Member States suggests that Slovakia's response, though immediate and robust, must evolve into a more systemic transformation. Strengthening the renewable energy sector, enhancing energy efficiency, reducing regional disparities, and improving institutional effectiveness are not only essential prerequisites for sustainable economic recovery but also key determinants of strategic resilience in an increasingly volatile global environment.

Furthermore, Slovakia´s economic model requires recalibration of its industrial base and labor market to better align with the principles of sustainability and digital transformation. Targeted investments in innovation, workforce upskilling, and inclusive regional development can support this transition and improve the country´s positioning within the evolving European economic framework. Cooperation with EU partners, effective utilization of recovery funds, and commitment to long-term fiscal discipline will be crucial for ensuring economic sovereignty, competitiveness, and resilience to future shocks.

In sum, the current crisis represents not only challenges but also a strategic opportunity. If appropriately managed, Slovakia's transition towards a greener, more resilient, and innovation-driven economy can lay the foundation for long-term prosperity and stability.

LITERATURE AND INFORMATION SOURCES USED

1. BLANCHARD, O. (2017). *Macroeconomics* (7th ed.). Pearson.

2. BRUEGEl. (2022). *Reducing EU dependency on Russian gas*. Retrieved from https://www.bruegel.org.

3. EUROPEAN COMMISSION. (2023). *REPowerEU Plan: Accelerating the clean energy transition*. Brussels: European Commission.

4. EUROPEAN COMMISSION. (2023b). *Cohesion policy and energy crisis: Regional impacts and responses*. Brussels: European Commission.

5. EUROPEAN COUNCIL. (2023). *Joint energy procurement and strategic storage initiatives.* Brussels: European Council.

6. ENERGY COMMUNITY. (2022). *Annual Implementation Report 2021–2022*. Vienna: Energy Community Secretariat.

7. EUROSTAT. (2021–2023). *Energy prices and consumption statistics.* Luxembourg: Eurostat. Retrieved from https://ec.europa.eu/eurostat

8. EUROSTAT. (2023b). *Natural gas consumption statistics (August 2022 – January 2023)*. Luxembourg: Eurostat.

9. INTERNATIONAL ENERGY AGENCY (IEA). (2022). *Energy Policy Review: Slovakia 2022*. Paris: IEA.

10. INTERNATIONAL ENERGY AGENCY (IEA). (2023). *Renewables and energy security in Europe*. Paris: IEA.

11. INTERNATIONAL MONETARY FUND (IMF). (2023). *Fiscal support during the energy crisis in Europe*. Washington, DC: IMF.

12. MACROTRENDS. (2023). *Gas and electricity price indices 2018–2023*. Retrieved from https://www.macrotrends.net

13. MINISTRY OF FINANCE OF THE SLOVAK REPUBLIC. (2023). *State Budget Report 2022*. Bratislava: MF SR.

14. NATIONAL BANK OF SLOVAKIA (NBS). (2023). *Macroeconomic Forecast for Slovakia 2023–2025*. Bratislava: NBS.

15. OECD. (2023). *Slovak Republic Economic Survey 2023*. Paris: OECD Publishing.

16. OECD. (2023b). *OECD Skills Outlook 2023: Skills for a resilient green economy*. Paris: OECD Publishing.

17. PUNTÍKOVÁ, L. – KOTEK, V. – ŠEBOVÁ, L. (2023). *Energy Security and Gas Imports in Central Europe: Post-2022 Trends**. Central European Energy Review, 15(1), 45–62.

18. SAMUELSON, P. A. – NORDHAUS, W. D. (2010). *Economics* (19th ed.). McGraw-Hill Education.
19. STATISTICAL OFFICE OF THE SLOVAK REPUBLIC. (2021). *Energy Balance of the Slovak Republic 2021*. Bratislava: ŠÚ SR.
20. STATISTICAL OFFICE OF THE SLOVAK REPUBLIC. (2023). *Inflation and Consumer Price Index Reports 2022–2023*. Bratislava: ŠÚ SR.
21. WORLD BANK. (2023). *Slovakia Country Economic Memorandum: Navigating Structural Shifts*. Washington, DC: World Bank Group.
22. YERGIN, D. (2006). *Ensuring Energy Security*. Foreign Affairs, 85(2), 69–82.

ADDRESS & ©

PhDr. Simona KOVÁČOVÁ, PhD.
Assistant Professor,
Matej Bel University, Faculty of Political Science and International Relations,
Kuzmányho 1, 974 01 Banská Bystrica,
Slovak Republic
simona.kovacova@umb.sk

Mgr. Martin JARABÁK
external doctoral student
Faculty of Public Policy and Public Administration
Danubius University
Fučíkova 269, 92521 Sládkovičovo,
Slovak Republic
jarabakm@centrum.sk

VEŘEJNÁ SPRÁVA, ŘÍZENÍ • PUBLIC ADMINISTRATION, MANAGEMENT

DOI: 10.36682/a_2025_2_5

CORRUPTION IN SLOVAK HEALTHCARE AS A RESULT OF SYSTEMIC FAILURES IN PUBLIC POLICY

Korupcia v slovenskom zdravotníctve ako dôsledok systémových zlyhaní verejnej politiky

Dušan MASÁR – Michal MOŽÍŠEK

Sládkovičovo, Slovak Republic

ABSTRACT: The aim of this paper is to generally analyze the phenomenon of corruption in the Slovak healthcare system as a manifestation of systemic deficiencies in public policy. It focuses on identifying the forms and extent of corruption, examining public and healthcare professionals' perceptions and personal experiences, and evaluating the impact of corrupt practices on public trust in state healthcare institutions. Based on these findings, the paper seeks to propose recommendations aimed at increasing transparency and efficiency within the Slovak healthcare system.

Key words: corruption – healthcare – public policy – transparency – failure

ABSTRAKT: Cieľom tohto príspevku je všeobecne analyzovať fenomén korupcie v slovenskom zdravotníctve ako prejav systémových nedostatkov verejnej politiky. Príspevok sa zameriava na identifikáciu foriem a rozsahu korupcie, skúmanie vnímania a osobných skúseností verejnosti a zdravotníckych pracovníkov, ako aj na hodnotenie vplyvu korupčných praktík na dôveru verejnosti v štátne zdravotnícke inštitúcie. Na základe zistených skutočností sa príspevok snaží navrhnúť odporúčania, ktoré by mohli prispieť k zvýšeniu transparentnosti a efektívnosti slovenského zdravotníckeho systému.

Kľúčové slová: korupcia – zdravotníctvo – verejná politika – transparentnosť – zlyhanie

---

INTRODUCTION

In the context of public policy, systemic deficiencies represent the fundamental framework within which conditions for the emergence and proliferation of corruption are formed, particularly in highly regulated and state-governed sectors such as healthcare. From a political science perspective, these deficiencies refer to structural and institutional weaknesses of the system that undermine the effectiveness of control mechanisms, reduce the transparency of decision-making processes, and create opportunities for the misuse of public resources for

personal gain. In the Slovak healthcare system, such deficiencies manifested, for example, in unclear financing rules, insufficient accountability of key actors, an inadequate system of remuneration, and limited capacities of control bodies, which are often unable to effectively prevent or detect corrupt practices.

Theories of public administration and public policy frequently emphasize that corruption, in such cases, is not merely a matter of individual misconduct but rather a symptom of deeper systemic problems embedded in the institutional arrangements and governance processes. In the Slovak healthcare sector, systemic deficiencies not only increase the risk of corruption but also hinder the implementation of effective anti-corruption measures. Without comprehensive institutional reform, improved transparency, and strengthened mechanisms of control and accountability, a significant reduction in corrupt practices, which undermine both the quality of healthcare services and public trust in the public sector, cannot be expected. This perspective aligns with analytical frameworks in public policy that emphasize the need for systemic approaches to addressing corruption as a phenomenon with broad social and economic impact.

Corruption in public policy represents one of the most serious and complex challenges facing modern democratic societies. It negatively affects not only the functioning of state institutions but also the quality of life of citizens, perceptions of justice, and equal access to public services. In the context of Slovak healthcare, one of the key pillars of the welfare state, corruption constitutes a major obstacle to the provision of effective, accessible, and high-quality healthcare. Systemic deficiencies in this sector, often rooted in historical, economic, and political factors, create fertile ground for the development of corrupt practices that erode public trust, diminish the moral integrity of institutions, and reduce the overall efficiency of service delivery.

This paper provides an empirical perspective on corruption as a manifestation of systemic failures in public policy, with a specific focus on the Slovak healthcare system. Its aim is to analyse the consequences of corruption for the public and state institutions, while also proposing potential solutions and measures aimed at increasing the transparency, efficiency, and credibility of the healthcare system. The paper primarily draws on the authors' original research. Prior to presenting the conclusions and findings of our study, the concept of corruption is briefly clarified. The analysis then proceed to the results of a questionnaire survey and propose recommendations for mitigating the negative trend of corruption.

METHODOLOGY AND OBJECTIVE

The objective of this paper is to examine of corruption in the Slovak healthcare system from the perspective of citizens, including their personal experiences with corrupt practices, and to analyze the consequences of corruption on trust in public healthcare institutions, willingness to use state healthcare facilities and the overall effectiveness of implemented public healthcare policy. Within the framework of the research conducted, four basic research questions were formulated to define the substantive focus of the questionnaire survey.

- How do citizens of the Slovak Republic perceive the presence of corruption in healthcare and what are their experiences with specific forms of corrupt behavior (e.g. informal payments, gifts, preferential treatment of patients)?
- To what extent does personal experience with corruption affect citizens' trust in public healthcare institutions and services provided by the state?
- Are there regional differences in the perception of corruption depending on the region, especially among citizens living in areas with lower quality and accessibility of healthcare infrastructure?
- What factors influence citizens' decision-making between public and private healthcare, and does the perceived incidence of corruption play a significant role in this process?

Based on the above questions, two main research hypotheses were formulated and subsequently tested through a questionnaire survey:

Hypothesis 1: In regions with lower quality of healthcare infrastructure, the perceived level of corruption in healthcare is higher.

Hypothesis 2: Personal experience with corruption increases the likelihood that individuals will prefer private healthcare providers over public ones.

The methodological approach of the study was based primarily on a questionnaire survey, which was deliberately distributed among diverse target groups in order to capture a broad range of perspectives on corruption in healthcare. The primary group of respondents consisted of citizens and patients, who were invited to complete the questionnaire via an online form disseminated through social media networks, including thematic groups focused on healthcare and health workers. To broaden the reach and heterogeneity of the sample, the "snowball" sampling method was also used, which allowed respondents to share the questionnaire within their social and professional networks. Another important target group of respondents comprised healthcare professionals, including physicians, nurses and other healthcare workers. These participants were approached through internal communication channels, personal contacts, as well as specialized online forums and discussion groups. In some

cases, specific healthcare facilities participated in the research, which enabled anonymous data collection among their employees, which increased the quality and relevance of the data obtained. In addition, the questionnaire was distributed to selected patient-rights organizations and civic associations, such as the *League for Mental Health* and the *Association for the Protection of Patient Rights*, which shared the questionnaire with their members or published it on their communication platforms. A significant group of respondents included university students enrolled in programmes related to public policy, social work and public health. Their participation provided insights from a younger generation with different value approach to corruption. Thanks to the targeted and diverse distribution of the questionnaire, it was possible to obtain a representative and diverse data set, which allows for a multidimensional analysis of corruption in the Slovak healthcare system and provides a valuable basis for formulating recommendations aimed at improving the transparency, trust and efficiency of public policy in this sector.

In addition to the questionnaire survey, the paper also used a descriptive method and the method of analysis and synthesis of knowledge, which enabled a comprehensive evaluation and integration of available empirical data with theoretical foundations from the field of public policy and healthcare. Thanks to these methods, it was possible to identify causal relationships and contextualize the research results within a broader framework of public policy processes.

THEORETICAL APPROACHES TO CORRUPTION AND THEIR REFLECTION IN PUBLIC POLICY

Before moving on to the research part focusing on corruption in the healthcare sector, this paper addresses the essence of this undesirable phenomenon from a theoretical perspective. The theoretical foundations of corruption as a public policy phenomenon are anchored in interdisciplinary research encompassing political science, public administration, law, economics and sociology. In political science discourse, corruption is perceived primarily as a violation of the normative framework governing the exercise of public power, whereby public officials abuse entrusted competencies to PURSUE private interests, thereby violating the principles of democratic legitimacy, the rule of law and equality before the law. The basic theoretical framework of corruption in the context of public policy was formulated by Robert Klitgaard, who presented the well-known model in his work *Controlling Corruption* (1988):

Corruption = Discretionary Power + Monopoly Power – Accountability.

According to Klitgaard, corruption occurs when an official has discretionary power, operates in an environment without competition, and lacks effective oversight or sanctions. The model has become the basis for the design of anti-corruption policies, especially in the areas of public procurement, administrative procedures, and licensing (Klitgaard, 1988).

From the perspective of institutional analysis, James C. Scott contributed to the theory of corruption, arguing in his work *Comparative Political Corruption* (1972) that corruption is a socially constructed phenomenon that can be implicitly tolerated as part of the informal system of power in some regimes. He draws attention to the differences between formal rules and actual political practice, while perceiving corruption as an indicator of the weak overlap of the rule of law in the exercise of public power. In analytical frameworks of public policy, corruption is often classified as a policy failure, where policy goals deviate from the public interest to particular interests due to information asymmetry, clientelism or state capture (Scott, 1972).

The approach outlined is developed by authors such as Hellman, Jones and Kaufmann (2000), who describe how economic and political elites systematically influence policy-making in favor of narrow groups (Hellman, Jones, Kaufman, 2000). Another key author is Susan Rose-Ackerman, who, in her work *Corruption and Government: Causes, Consequences, and Reform* (1999), analyzes corruption as a structural problem of public institutions. According to her, corruption is not only a question of individual morality, but mainly of the systemic setting of rules and incentives. She proposes reforms based on transparency, rationalization of bureaucracy and participatory decision-making. Rose-Ackerman distinguishes between "petty" and "grand" corruption and points out their different mechanisms and consequences for public policy (Rose-Ackerman, 1999).

In the European context, Alina Mungiu-Pippidi has played a significant role in focusing on corruption as a normative deficit in society. In her book *The Quest for Good Governance: How Societies Develop Control of Corruption* (2015), she argues that the key to reducing corruption is not only laws, but a cultural transformation of society towards norms of public integrity. She emphasizes the importance of active citizenship, open government and independent media.

In Slovakia, Emília Sičáková-Beblavá has long been engaged in corruption research. In several publications, such as *Korupcia a protikorupčná politika na Slovensku* (Corruption and Anti-Corruption Policy in Slovakia) (2003), *Transparentnosť a verejná kontrola* (Transparency and Public Control) (2004), she analyzed the relationship between insufficient transparency in public administration, weak control of public spending and the spread of corrupt practices. She

also focused on the development of public control mechanisms and participatory tools as a means of increasing the resilience of public policies to corruption. As she states, "*Corruption is an expression of a weak system of public control, where the absence of transparency supports the emergence of informal rules of the game*" (Sičáková-Beblavá, 2004, p. 42). Corruption can take many forms, ranging from informal payments for routine medical services and preferential treatment of patients to systemic violations of ethical and legal standards in procurement, the allocation of public funds, or personnel management. As Klitgaard states, "*corruption arises where monopoly of decision-making, discretionary power, and low accountability meet*" (Klitgaard, 1988, p.27).

Healthcare, as a sector characterized by high levels of public expenditure and, at the same time, a low level of control over financial flows, appears to be particularly susceptible to corrupt practices. According to several studies by Transparency International Slovakia, healthcare ranks among the three most corrupt areas of the public sector in Central and Eastern European countries. The so-called asymmetry of information between doctors and patients also plays a significant role here, which allows for the distortion of standard ethical norms and the penetration of informal mechanisms into the normal operation of the system. Corruption is a complex social phenomenon that can manifest itself through various forms and mechanisms. Its classification takes into account not only the scope and level at which it occurs, but also the method of implementation, the nature of the relationships between the involved actors and the underlying motivation. Such a systematic categorization allows for a deeper understanding of the dynamics of corrupt behavior and its embeddedness in public policy. In terms of the scope and level of occurrence, corruption is most commonly distinguished as grand, petty and systemic corruption. Grand corruption is concentrated at higher levels of public power and typically involves political elites, strategic decisions related to public procurement, legislative processes, or privatization. It has a strongly systemic character, which fundamentally affects the efficiency of public administration and the management of public finances. By contrast, petty corruption is linked to everyday interactions between citizens and public administration (Meričková, Majerík, Lendvorský, 2021). Such practices are common, for example, in healthcare, education or traffic policing, where they manifest in the form of unofficial payments, gifts or attempts to speed up administrative processes. A particularly serious form is systemic corruption, which permeates the entire structure of public institutions, becomes an integral part of their normal functioning, is predictable and socially tolerated. In such an environment, clientelistic networks emerge, involving interconnected officials, suppliers and political actors.

With regard to forms and methods of implementation, corrupt behavior can be categorized according to the specific mechanisms through which it is carried out. Bribery is the most classic form of corruption, consisting in providing or receiving money or other benefits in order to influence the decision-making of a public official. Related forms include clientelism and nepotism, which involve favoring political allies, family members or acquaintances in the allocation of positions, public contracts or subsidies regardless of expertise and objective criteria. Another significant manifestation of corruption is the abuse of power, defined as the deliberate violation of legal obligations by a public official for personal or political gain, typically exemplified by the manipulation of public procurement processes. Conflict of interest is also closely linked to corruption, which arises when a public official finds themselves in a situation where personal interests may compromise the impartiality and objectivity of the performance of their public duties. A special category is represented by informal payments, often referred to as "unofficial fees", which, although not legally required, have become normalized, especially in the healthcare sector (Konečný, 2021).

Another aspect of corruption classification concerns the nature of the relationships between the parties involved. Vertical corruption occurs between a citizen (or business entity) and a public official or political representative, with a typical example being the provision of a gift to a doctor in exchange for faster access to healthcare services. Horizontal corruption occurs between actors at the same institutional level, such as hospitals and suppliers and often involves price manipulation or collusive arrangements leading to overpriced purchases. Internal corruption refers to corrupt practices occurring within an institution itself, involving its own employees. Finally, in terms of motivation and purpose, a distinction can be made between coercive corruption and proactive corruption. Coercive corruption arises when a public official demands a bribe as a condition for performing a duty that should otherwise be carried out without any illict compensation. In contrast, corruption on the initiative is characterized by voluntary cooperation between both parties, with the aim of circumventing legal regulations or obtaining an unjustified advantage, typically in the case of manipulation of public procurement.

One of the most striking systemic indicators of corruption is a low level of transparency in decision-making processes, which creates space for clientelism and uncontrolled influences. Corruption most often appears in environments where decision-making lacks transparency and citizens do not have the opportunity to effectively control the exercise of power (Klitgaard, 1988). Under conditions in which control and oversight bodies are formally established but fail to perform their function, corruption becomes a systemic phenomenon. An independent judiciary, an effective prosecutor's office, the Supreme Audit Office or anti-corruption agencies

are key tools for limiting corruption, but their dysfunctionality creates a "green zone" for impunity. As Karkalík notes, *"corruption flourishes where institutions are weak, understaffed or politically influenced."* (Karkalík, 2010, p. 89). When legislation is unclear, subject to frequent changes or allows for broad interpretation, a legal environment conducive to subjective decision-making emerges. This situation leads to selective application of rules, which in turn provides fertile ground for corrupt agreements. Political control over authorities that should operate independently (e.g., public procurement authorities, health insurance companies, supervisory boards) creates the prerequisites for systemic clientelism. A high degree of politicization within public administration results in the informal control of public resources and reduces the accountability of public officials.

CORRUPTION AS A SYSTEMIC FAILURE OF PUBLIC POLICY IN THE SLOVAK HEALTHCARE SYSTEM

As part of the research, the methodological procedure of which was outlined at the beginning of the article, a total of 550 questionnaires were distributed. Of the total number, 224 completed questionnaires were returned, which represents a response rate of approximately 40.7%. After excluding incomplete or evidently frivolous responses, 212 valid questionnaires were included in the subsequent analysis. The collected data were processed using descriptive statistics (frequencies, percentage distributions), basic cross-sectional analyses (e.g. examining the relationship between demographic characteristics and attitudes towards corruption), and space was also left for the analysis of open-ended responses, which provided valuable illustrative insights. The results of the questionnaire survey indicate that the quality of healthcare infrastructure significantly influences the perception of corruption within the Slovak healthcare system. As many as 68% of respondents from regions with lower-quality infrastructure assessed the condition of healthcare facilities as insufficient or poor. Among these respondents, 74% reported perceiving the occurrence of corrupt practices, such as unofficial payments and preferential treatment of patients, as a common phenomenon in their region. Overall, 57% of all respondents stated that they had personal experience with corruption in the healthcare sector. Of these, 82% reported that such experiences had negatively affected their trust in the provision of services in public healthcare facilities. This loss of trust was also reflected in healthcare preferences when choosing healthcare, as 63% of respondents with personal experience of corruption expressed a preference for using private healthcare services in the future. When asked about the frequency with which corruption affects the quality of healthcare provision, 58% of respondents from regions with weaker infrastructure reported that

this occurred regularly or often. By contrast, only 23% of respondents from better-equipped regions reported similar perceptions, which supports the hypothesis that poorer healthcare infrastructure is associated with higher perceived levels of corruption.

Respondents also expressed the view that a consistent fight against corruption would significantly increase trust in public healthcare, with 79% of respondents agreeing with this statement. Regarding the conduct of healthcare personnel, 61% of respondents from regions with weaker infrastructure reported perceiving unfair or unequal treatment of patients, which they associated with corrupt practices. The most frequently proposed measures to reduce corruption included increasing the transparency of processes (suggested by 68% of respondents), strengthening oversight of healthcare facilities (64%) and improving the financing of infrastructure (59%). These measures correspond with the need to strengthen the basic conditions for the effective functioning of the healthcare system. Finally, 71% of respondents perceived private healthcare facilities as providing higher-quality and more reliable services than public ones, which aligns with their tendency to prefer the private sector following negative experiences with corruption. At the same time, 54% of respondents reported having at least occasional access to private healthcare services, indicating that despite the preference for public healthcare services, the private sector often represents a sought-after alternative.

The findings clearly indicate that demographic factors influence both the perception of corruption in healthcare and responses to it, suggesting that anti-corruption measures should take into account the age, gender, and educational structure of the population. The highest share of personal experience with corruption was observed in the 30-44 (65%) and 45-59 (70%) age groups. In contrast, the lowest share was observed among younger respondents aged 18-29 (40%) and seniors aged 60 and over (50%). These results may indicate that individuals of working age use healthcare services more frequently and are therefore more likely to encounter corrupt practices.

With regard to the impact of personal experience with corruption on trust in public healthcare from a gender perspective, the findings indicate that women reported a more pronounced decline in trust (85%) compared to men (75%). This difference may be associated with a stronger perception of injustice or a greater sensitivity among women to manifestations of systemic inequality.

Findings concerning preferences for the healthcare sector following personal experience with corruption, differentiated by education level, show that while the share of respondents preferring the private sector among those with primary education was evenly balanced (50%), it increased to 60% among respondents with secondary education and reached 75% among

those with university education. Higher education attainment is likely associated with greater expectations regarding service quality and transparency, as well as the financial capacity to access private healthcare services.

The most important findings of the research can be summarized in four points:

- Personal experience with informal payment: the majority of respondents (57%) reported having personal experience with corruption.
- Impact on trust: among those with personal experience, 82% reported a negative impact on trust in the public healthcare system.
- Preference for the private sector: 63% of respondents with personal experience of corruption expressed a preference for private healthcare facilities.
- Perception of corruption by region: in regions with weaker infrastructure, corruption is perceived as more frequent (58%) than in better-equipped ones (23%).

Based on the research results, several measures can be proposed that could contribute to limiting corrupt practices in the Slovak healthcare system and increasing public trust in it.

First, it is necessary to increase transparency in the processes and financing of healthcare facilities. The introduction of mandatory publication of waiting lists, contracts with health insurance companies, results of internal audits or hospital income figures can contribute to the creation of a controllable and transparent environment, thereby limiting the scope for informal agreements. Digitalization of administrative processes also plays an important role, as it can reduce direct contact between patients and staff when arranging procedures or appointments, thereby reducing the risk of "envelope motivation".

Another important measure is to make control and sanction mechanisms more effective. It is necessary to strengthen independent bodies or internal departments within healthcare facilities that are responsible for investigating suspicions of unethical or corrupt behavior. The introduction of anonymous reporting of corruption is currently possible, but it is not widely used in practice. Consistent verification of complaints could strengthen citizens' trust in the fairness of the system and, at the same time, reduce the level of tolerance towards informal payments.

An equally important factor is the increase in the salary and overall working conditions of healthcare personnel. If healthcare workers are not provided with adequate and fair financial remuneration, they may be motivated to seek additional income through informal channels. In addition to wage policy, it is also important to ensure opportunities for professional growth, continuous education and job stability. Ethical and legal education also plays an important role in prevention. Meaningful educational campaigns that address patients' rights, procedures for

filing complaints and the possibility of defending oneself against unethical behavior can contribute to changing public attitudes. At the same time, it is necessary to strengthen the teaching of ethics, professional conduct and anti-corruption principles in the training of future healthcare professionals.

An important area that directly affects perceptions of the fairness in the healthcare system is the equal availability of quality services across regions. The research results showed that corruption is perceived as more frequent in areas with poorer infrastructure. Investment in the modernization of regional hospitals, better staffing and quality equipment can reduce patients' dependence on informal mechanisms of "preferential" access. Another suitable tool is the introduction of a system of regular patient satisfaction assessments. Transparent and publicly available evaluations of service quality create pressure for raising standards, while also allowing patients to provide feedback that serves as an indicator of the ethics and professionalism of a particular facility.

Finally, to enhance transparency, it would be desirable to publish information on conflicts of interest and donations received by health professionals or healthcare facilities. This measure would help to limit the potential influence of pharmaceutical companies or other commercial entities on the decision-making of health personnel and at the same time strengthen public confidence in the independence of healthcare.

In the Slovak context, corruption in healthcare has long been identified as one of the most problematic phenomena in the public service sector. In addition to the present research, evidence of the persistent occurrence of corruption is provided by both subjective assessments (e.g. public surveys, experiences of patients and healthcare professionals) and objective data from audit reports of the Supreme Audit Office, investigative findings in the media and analyses by non-governmental organizations. The causes of this situation are deeply rooted in systemic shortcomings of public policy, which can be identified at several levels:

Institutional level: healthcare institutions often exhibit weak governance and accountability. Insufficient control over decision-making processes, weak oversight of public spending, low transparency in procurement and conflicts of interest between managers and suppliers lead to the creation of an environment prone to abuse.

Legislative level: Although health policy legislation includes formal anti-corruption measures (e.g. conflict of interest law, public procurement laws), their implementation is inconsistent and often insufficiently enforced. Systemic preventive tools such as codes of ethics, internal controls or support for whistleblowing within hospitals and other healthcare providers are also lacking.

Organizational level: Decentralized hospital management, the absence of a unified strategy to combat corruption in healthcare, and the politicization of management positions create space for clientelistic networks that retain power despite changes in political representation.

Value level: Social tolerance of informal payments, the historical legacy of a "gift" culture, and poor awareness of patients' rights contribute to the reproduction of corruption mechanisms. The public often perceives bribery as a necessity for securing quality care, which legitimizes unfair practices and weakens collective awareness of the need for systemic change.

Given the above, it can be stated that corruption in healthcare is not only the result of individual misconduct, but also reflects deeper failures in public policy, which concern not only its content and goals, but especially the manner in which these goals are implemented. Therefore, addressing corruption is not merely a matter of sanctioning specific perpetrators, but also of reforming the institutional environment, legislative framework, organizational culture and values embodied by public policy in the healthcare sector. Corruption in healthcare should be viewed as a mirror of public policy, i.e., an indicator of the extent to which public administration is able to resist pressures, manage conflicts of interest and maintain a balance between public interest and individual benefit. Resistance to corruption should be understood as an integral component of the quality of public policy, not only in terms of the efficiency of public resource use, but also in terms of the legitimacy of the state as a guarantor of justice and credibility in the eyes of citizens.

CONCLUSION

Public policy is a complex and multi-layered process through which public institutions, often in collaboration with diverse actors, including political leaders, experts, civil society and the private sector, respond to societal challenges and shape the development of individual areas of public life. In the context of healthcare, public policy plays an irreplaceable role, as it determines the frameworks of financing, regulation, accessibility and quality of healthcare services. Failures in this process can lead to serious consequences not only at the individual level, but also within the broader system of service provision. One of the most striking manifestations of ineffective public policy is corruption, which is perceived as an extremely sensitive and socially significant phenomenon in healthcare. Corruption involves the abuse of public power or position for personal gain, thereby eroding citizens' trust in justice, equality and the functionality of the public sector. The fight against corruption in public policy is a complex and long-term process that goes beyond repressive measures and affects the very

structure of the functioning of the state, public administration, legislation and civil society. Corruption is not only an individual failure, but also a manifestation of institutional weaknesses, legal uncertainty and distorted norms of political culture. Therefore, an effective fight against corruption is conditional on systematic reforms that include strengthening the transparency, accountability and effectiveness of public institutions, as well as creating an environment with low tolerance for unethical behavior.

The present research has shown that corruption in the Slovak healthcare system is perceived as a widespread phenomenon. The majority of respondents (84%) stated that corruption occurs frequently or occasionally, indicating a strongly negative perception of the healthcare system among citizens. At the same time, almost half of the respondents (48%) confirmed that they had personally encountered an unofficial request for payment or a gift in the healthcare system, which highlights the link between perceived corruption and patients´ actual experience. Although the majority of respondents oppose such practices, 39% admitted a certain degree of justification for unofficial payments or gifts to doctors, suggesting that tolerance towards corruption remains relatively high in certain segments of the population. This may result from long-term distrust in official procedures, which is also reflected in the low level of public trust in state healthcare institutions. The average level of trust was 2.4 on a five-point scale, with respondents most often reporting a trust level of 2.

The research showed that the perception of corruption in the healthcare sector in Slovakia is widespread and significantly influenced by the quality of healthcare infrastructure in individual regions. Respondents from regions with weaker, outdated or insufficient infrastructure reported significantly more frequent occurrence of corrupt practices compared to those from areas with better healthcare facilities. This finding confirms Hypothesis 1, indicating that perceived corruption is higher in regions with poorer-quality healthcare infrastructure.

Another significant finding is the impact of personal experience with corruption on patient preferences. Respondents who had encountered corrupt practices, such as unofficial payments or requests for donations in the healthcare sector, were more likely to prefer using private healthcare facilities. Over 60% of respondents with such experience reported preferring private alternatives due to a loss of trust in the public healthcare system, which supports Hypothesis 2. The trend suggests that corruption can have a negative impact not only on trust in state institutions, but also on the choice of healthcare provider.

Moreover, respondents from regions with lower-quality infrastructure also expressed a higher level of dissatisfaction with public health services, which may contribute to a poorer overall image of the healthcare system. In this context, corruption appears as an additional

factor that exacerbates an already tense situation and leads to reduced trust in state health facilities. The data obtained thus confirm that the quality of healthcare infrastructure and personal experience with corruption significantly influence both the perception of corruption and citizens' decisions regarding the use of public or private healthcare services. The results also indicate the need for systemic measures to improve infrastructure alongside a more consistent fight against corruption in order to increase public trust in the state health system.

In the open-ended part of the questionnaire, respondents most frequently proposed solutions focused on systemic changes. The most common recommendations included increased transparency and digitalization, such as public overviews of waiting lists, stricter sanctions for perpetrators, higher salaries for healthcare workers, stronger control and external oversight, and the introduction of anonymous systems for reporting corruption.

In summary, the research confirmed that corruption is perceived as a widespread problem with a significant impact on citizens' trust in the healthcare system. Tolerance towards these practices remains relatively high among a portion of the population, particularly among those who have had personal experience with corruption. Citizens view the solution primarily in fundamental systemic measures that would increase transparency and strengthen the effectiveness of anti-corruption efforts in public healthcare.

REFERENCES AND INFORMATION SOURCES USED

1. HELLMAN, J. S. – JONES, G. – KAUFMAN, D. (2000). *Seize the State, Seize the Day-State Capture, Corruption, and Influence in Transition* (s. 1-37). Policy Research Working Paper 2444, The World Bank Institute Governance, Regulation, and Finance Division and Europe and Central Asia Region Public Sector Group and European Bank of Reconstruction and Development Office of the Chief Economist. https://doi.org/10.1596/1813-9450-2444.

2. KARKALÍK, J. (2010). *Korupcia ako spoločenský fenomén*. Brno: Masarykova univerzita, 156 s., ISBN 9788021051380.

3. KLITGAARD, R. (1988). *Controlling Corruption.* Berkeley: University of California Press, 306 s., ISBN 9780520079119.

4. KLITGAARD, R. (1988). *Corruption Across Countries and Cultures*. Lee Kuan Yew School of Public Policy Research Paper No. 17-23, http://dx.doi.org/10.2139/ssrn.3035100.

5. KONEČNÝ, S. (2021). *Teória verejnej politiky*. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, Šafárik Press, 2021. 242 s., ISBN 978-80-574-0011-0.

6. MIKUŠOVÁ MERIČKOVÁ, B. – MAJERÍK, M. – LENDVORSKÝ, M. (2021). *The problem of corruption in the contracting out of public services – the case of Slovakia.* Acta

Universitatis Bohemiae Meridionalis, Vol 24, No 2 (2021), 24(2):75-90. https://doi.org/10.32725/acta.2021.008.

7. MUNGU-PIPPIDI, A. (2015). *The Quest for Good Governance: How Societies Develop Control of Corruption* https://doi.org/10.1017/CBO9781316286937.

8. ROSE-ACKERMAN, S (1999). *Corruption and Government: Causes, Consequences, and Reform*. Cambridge University Press. https://doi.org/10.1017/CBO9781139175098.

9. SIČÁKOVÁ-BEBLAVÁ, E. – ZEMANOVIČOVÁ, D. (2003). *Korupcia a protikorupčná politika na Slovensku v roku 2003*. Bratislava: Transparency International Slovensko, 266 s., ISBN 80-89041-74-4.

10. SIČÁKOVÁ-BEBLAVÁ, E. (2004). *Transparentnosť a verejná kontrola*. Bratislava: Transparency International Slovensko, 128 s., ISBN 8089215199.

11. SCOTT, J. C. (1972). *Comparative Political Corruption.* New Jersey: Prentice-Hall, Englewood Cliffs, 166 s., ISBN 0131539248.

ADDRESS & ©

doc. Ing. Dušan MASÁR, PhD.
Associate Professor
Faculty of Public Policy and Public Administration
Danubius University
Fučíkova 269, 92521 Sládkovičovo,
Slovak Republic
dusan.masar@gmail.com

Ing. Michal MOŽÍŠEK
external doctoral student
Faculty of Public Policy and Public Administration
Danubius University
Fučíkova 269, 92521 Sládkovičovo,
Slovak Republic
doktorandivpvs@azet.sk

RECENZNÍ ŘÍZENÍ PRO Č. 2/2025

Jednotliví oponenti (9) recenzovali 1–2 články. Redakce od nich obdržela na každý příspěvek 1–2 posudky, celkem 12 posudků.

doc. JUDr. PhDr. Jiří **BÍLÝ**, CSc.	Katedra právních oborů a bezpečnostních studií, Vysoká škola evropských a regionálních studií z. ú., České Budějovice, **ČR**
Ing. Monika **BŘEZINOVÁ**, Ph.D.	Katedra managementu veřejné správy, Vysoká škola evropských a regionálních studií z. ú., České Budějovice, **ČR**
PhDr. Jan **ČÁP**, Ph.D.	Katedra bezpečnosti a veřejného pořádku, Fakulta právních a správních studií, VŠFS Praha, **ČR**
doc. PaedDr. Zuzana **HORVÁTHOVÁ**, Ph.D.	Katedra právních disciplín a veřejné správy, Metropolitní univerzita Praha, **ČR**
doc. Ing. Radoslav **IVANČÍK**, PhD. et PhD., MBA	Katedra filozofie a politológie, Filozofická fakulta, Univerzita Konštantina Filozofa, Nitra, **SR**
Dr. h. c. prof. Ing. Pavel **NEČAS**, PhD.	Katedra bezpečnostních štúdií, Fakulta politických vied a medzinárodných vzťahov, Banská Bystrica, **SR**
doc. PhDr. Miroslav **SAPÍK**, Ph.D.	Katedra managementu veřejné správy, Vysoká škola evropských a regionálních studií z. ú., České Budějovice, **ČR**
JUDr. Marie **SCISKALOVÁ**, Ph.D.	Ústav veřejné správy a regionální politiky, Slezská univerzita v Opavě, **ČR**
doc. Ing. Jaroslav **SLEPECKÝ**, PhD., MBA	Katedra právních oborů a bezpečnostních studií, Vysoká škola evropských a regionálních studií z. ú., České Budějovice, **ČR**

POČET OBDRŽENÝCH VĚDECKÝCH ČLÁNKŮ:	8
POČET RECENZOVANÝCH VĚDECKÝCH ČLÁNKŮ:	6
POČET OBDRŽENÝCH RECENZNÍCH POSUDKŮ:	14
POČET PUBLIKOVANÝCH VĚDECKÝCH ČLÁNKŮ:	5

O ČASOPISU

Základní charakteristika

Časopis Auspicia je nezávislým recenzovaným vědeckým časopisem pro otázky společenských a humanitních věd. Obsah časopisu prezentuje původní vědecké příspěvky, které jsou orientované na stěžejní obory zaměření periodika a rovněž v současnosti významné a řešené problémy. Mnohé z nich podávají formou přehledových studií návrh na reálné řešení konkrétních problémů, polemik ve smyslu akademické plurality názorů.
Historicky je založen na 5 základních a respektovaných principech:

- řádné a přísné recenzní řízení;
- mezinárodnost;
- otevřenost;
- výběrovost;
- kontinuální zvyšování kvality.

Historie

Časopis Auspicia je vydáván od r. 2004 Vysokou školou evropských a regionálních studií (VŠERS) a Vysokou školou technickou a ekonomickou (VŠTE) dvakrát ročně, pouze elektronicky. V dosavadních 41 číslech bylo otištěno zhruba 860 příspěvků a recenzí.

Rada pro výzkum, vývoj a inovace jako odborný a poradní orgán vlády ČR zařadila časopis Auspicia (ISSN 1214-4967) pro léta 2008–2013 a znovu pro rok 2015 (http://www.vyzkum.cz/FrontClanek.aspx?idsekce=733439) mezi recenzované neimpaktované časopisy, které uvedla v oborech Národního referenčního rámce excelence (NRRE).

V roce 2016 byl recenzovaný vědecký časopis Auspicia zařazen do mezinárodní databáze ERIH PLUS a od roku 2024 do online knihovny pro střední a východní Evropu – CEEOL.

Tematické sekce

Na základě úspěšného recenzního řízení jsou jednotlivé vědecké příspěvky řazeny do sekcí:

1. Společenské vědy
2. Bezpečnost
3. Veřejná správa, řízení
4. Recenze

<u>Základní pokyny autorům</u>

Jazyk vědeckého příspěvku: angličtina, čeština; **recenze**: angličtina, čeština, Články mohou být psány v angličtině nebo češtině, ale vzhledem k mezinárodnímu rozměru časopisu jsou preferovány anglické články.

Požadovaný rozsah v sekcích 1–3: max.8 normostran (1NS – 1800 znaků včetně mezer).

Data uzávěrek: 1. číslo – 1. 2. • 2. číslo – 1. 8.

Použitá literatura: 25 % zdrojů indexovaných v databázích Web of Science a/nebo Scopus.

Recenzní řízení: oboustranně anonymní, nezávislé, objektivní.

Data vydání: 1. číslo – 1. 6. • 2. číslo – 1. 12.

Podrobný zdroj: https://vsers.cz/auspicia/
Jak citovat vědecký příspěvek: In.: Pro autora. Šablona článku – https://vsers.cz/auspicia/

Autorský poplatek: Za výdaje spojené s uveřejněním vědeckého příspěvku v českém jazyce (příspěvky v angličtině jsou do odvolání dočasně bezplatné) v délce **max. 8 normostran** v sekcích 1–3 hradí autor částku **1 000,- CZK** *(popř. částku zvýšenou o 200, - Kč za každou další normostranu)*, nebo příslušnou částku v EUR dle aktuálního přepočtu, a to nejpozději do uzávěrky příslušného čísla (tj. před recenzním řízením) převodem na účet vydavatele (VŠERS) u Fio banky, a. s. (pobočka České Budějovice) č. 2101783605/2010, účet EUR/IBAN: CZ71 2010 0000 0024 0178 3607, BIC kód: FIOBCZPPXXX (zahraniční plátci si poplatek za převod hradí sami), nebo v hotovosti na ekonomickém oddělení VŠERS. Variabilním symbolem je IČO autorova pracoviště a specifickým symbolem číselný kód 12342022. Do zprávy pro příjemce se uvede jméno autora / autorů a pracoviště.

Kontaktní adresa:
Vysoká škola evropských a regionálních studií, z. ú.
Žižkova tř. 1632/5b
370 01 České Budějovice
doc. PhDr. Miroslav Sapík, Ph.D.
Telefon: +420 386 116 839
E-mail: sapik@vsers.cz, https://vsers.cz/auspicia/

ABOUT THE JOURNAL

General description

Auspicia is an independent, peer-reviewed scientific journal on the social sciences and humanities. The journal presents original scientific contributions on core areas of its field of focus, as well as currently significant and solved problems. In the form of overview studies, many of them constitute proposals for a real solution to specific problems, polemics in the sense of academic plurality of opinions.

The journal is based on five respected principles:
- proper and rigorous review procedures;
- internationality;
- openness;
- selectivity;
- continuous improvement in quality.

History

Auspicia has been published since 2004 by the College of European and Regional Studies (VŠERS) and the Institute of Technology and Business (VŠTE) twice a year, in electronic form only. So far, 860 scientific contributions and reviews have been published in 42 issues.
The Innovation Council, being a professional and advisory board of the government of the Czech Republic, included *Auspicia* (ISSN 1214-4967) among reviewed, non-impact scholarly journals involved in the topics of the National Reference Framework of Excellence (NRRE) in 2008–2013, and it was included there again in 2015 (http://www.vyzkum.cz/FrontClanek.aspx?idsekce=733439).

In 2016 *Auspicia* was listed in the international database ERIH PLUS and since 2024, it has been listed in the Central and Eastern Europe Online Library – CEEOL.

Thematic sections

After individual scientific papers successfully pass review, they are allocated towards one of the following sections:

1. Social Sciences
2. Safety
3. Public Administration, Management
4. Reviews

Basic instructions for authors

Language of the scientific paper: English, Czech; **reviews**: English, Czech. Articles can be submitted in either English or Czech, but English articles are preferred due to the international dimension of the journal.

Required range in sections 1–3: maximum 8 standard pages (1 standard page – 1800 characters including spaces).

Deadlines: 1st issue – 1 February, 2nd issue – 1 August.

Bibliography: 25% of resources indexed in Web of Science and/or Scopus databases.

Review process: double-blind, independent, objective.

Publishing dates: 1st issue – 1 June, 2nd issue – 1 December.

Detailed source: https://vsers.cz/recenzovany-vedecky-casopis-auspicia

How to cite a scientific paper: In: For the author. Article template -

https://vsers.cz/vedecky-casopis-auspicia/

Author's fee. Authors of the papers (contributions) are to pay the amount of CZK 1,000 for the expenses connected with publishing the scholarly contributions in the Czech language (contributions in English are temporary free of charge until further notice) of a maximum of 8 standard pages (or that amount plus CZK 200 per each subsequent standard page), or the appropriate amount in EUR in accordance with the current exchange rate in sections 1–3. This must be done by the closing date of the relevant volume (i.e., before the review process) either by means of bank transfer to the publisher's bank account No. 2101783605/2010**,** at Fio Banka, a. s. (České Budějovice branch), account EUR/IBAN code: CZ71 2010 0000 0024 0178 3607, BIC code: FIOBCZPPXXX (foreign payors pay the transfer charge by themselves), or they may pay it in cash at the Department of Economics of the College of European and Regional Studies. Registration numbers of authors' workplaces are variable symbols, the specific symbol is a code with the following digits: 12342022. The information regarding the payee should include the name of the author/authors and their workplace.

Contact address:
The College of European and Regional Studies
Žižkova tř. 1632/5b
370 01 České Budějovice
doc. PhDr. Miroslav Sapík, Ph.D., editor-in-chief
Telephone number: +420 386 116 839
E-mail: sapik@vsers.cz, https://vsers.cz/auspicia/