ISSN 2669-2023 (print) / ISSN 2538-8959 (on-line) **/ https://doi.org/10.47459/cndcgs.2026.115**

Smart Technologies, Social Dynamics, and National Security

Erika FECKOVÁ ŠKRABUĽÁKOVÁ[1]*, Tomáš ŠKOVRÁNEK[1]

[1]Institute of Control and Informatization of Production Processes, Faculty of Mining, Ecology, Process Control and Geotechnologies, Němcovej 3, 04200 Košice, Slovakia

*Correspondence:*erika.feckova.skrabulakova@tuke.sk*

Abstract

The paper examines contemporary national defence challenges arising from the interconnection of digital technologies, social dynamics, and global tensions. Using interdisciplinary analysis and policy review, it explores how cyber threats and emerging technologies shape resilience and security outcomes. The findings highlight the critical role of societal trust, strategic communication, and coordinated international frameworks such as NATO and EU initiatives. The study implies that effective defence strategies require integrated technological, social, and policy dimensions. The paper contributes original insights into comprehensive security approaches that enhance both national and collective resilience in the digital age.

KEY WORDS: *national defence, cyber threats, artificial intelligence, societal resilience, disinformation, international cooperation, EU security initiatives, modern technologies*

Citation: Fecková Škrabuľáková, E.; Škovránek, T. Smart Technologies, Social Dynamics, and National Security. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 7-10 September 2026. ISSN 2669-2023, https://doi.org/10.47459/cndcgs.2026.115

1. Introduction

Modern technologies are reshaping not only the tools of national defence but also the social environment in which security policies operate. The interaction between technology and society has become a critical factor influencing resilience, stability, and the effectiveness of defence strategies.

Contemporary security environments are increasingly shaped by the dynamic convergence of technological innovation, societal transformation, and intensifying geopolitical tensions. The rapid development of digital technologies, particularly artificial intelligence (AI), the internet of things (IoT), big data analytics, and cloud computing, has fundamentally altered both the nature of threats and the mechanisms through which states ensure national defence and resilience. On the one hand, these technologies enable enhanced risk prediction, improved operational efficiency, and more informed strategic decision-making. On the other hand, they simultaneously expand the attack surface and create new vulnerabilities, as highly interconnected systems become attractive targets for sophisticated cyber and hybrid threats [1-3].

This transformation underscores that national security in the digital age is no longer solely a technological or military issue, but a multidimensional challenge encompassing legal, ethical, social, and political dimensions. The proliferation of smart infrastructures and smart city ecosystems illustrates this duality: while increasing efficiency, sustainability, and quality of life, they also introduce risks related to cyberattacks, data governance, and privacy protection [4-5]. Similarly, the application of big data and algorithmic tools in security practices, such as predictive analytics and policing, raises significant concerns regarding civil liberties, discrimination, and the balance between security and individual rights [1]. These developments highlight the necessity of critically examining not only the capabilities of emerging technologies but also their broader societal implications.

At the same time, the evolving security landscape challenges traditional, state-centric and military-focused conceptions of power. Contemporary understandings of national security emphasize a broader set of determinants, including technological capacity, governance quality, human capital, and societal trust. Security is increasingly perceived as the outcome of the interaction between "hard" and "soft" power elements, where education, innovation, and social cohesion play a decisive role in shaping a state's resilience and strategic position in the international system [6]. Moreover, technological innovation itself is no longer viewed merely as an instrument of power, but as an integral component of national identity and a key factor in sustaining economic and political systems [7].

Peer-review under responsibility of General Jonas Žemaitis Miltitary Academy of Lithuania and University of Defence, Czech Republic

Another critical dimension of this transformation is the growing importance of governance and strategic coordination in managing digital technologies [8-9]. The integration of advanced technologies into national security systems requires comprehensive frameworks that combine organizational, legal, and economic measures to ensure their effective and responsible use [10]. At the same time, the increasing "smartness" and interconnectedness of critical infrastructures introduce new systemic risks, including vulnerabilities stemming from centralization, automation, and interdependence, which may undermine resilience if not properly addressed [5]. These challenges highlight the need for adaptive and forward-looking strategies capable of responding to rapidly evolving threat landscapes.

Equally important is the role of international cooperation in addressing security challenges that transcend national borders. Cyber threats, technological competition, and global interconnectivity necessitate coordinated responses and shared frameworks among states and international organizations. Collaborative initiatives contribute to the development of common standards, information sharing, and collective resilience, while also reflecting the competitive dimension of technological advancement in global politics [2-3]. In this context, security becomes not only a national concern but also a collective endeavour embedded in broader international structures.

In response to these developments, this paper adopts an interdisciplinary perspective to examine how the interconnection of digital technologies, social dynamics, and global tensions shapes contemporary national defence challenges. It focuses on the impact of cyber threats and emerging technologies on security outcomes, while emphasizing the critical role of societal trust, strategic communication, and coordinated policy frameworks. By integrating technological, social, and policy dimensions, the study aims to provide a comprehensive understanding of security in the digital age, particularly how the interaction between digital technologies and social dynamics reshapes national defence, with a focus on societal resilience, trust, and security outcomes. It also offers insights for the development of effective and resilient defence strategies.

Given the complexity and rapidly evolving nature of smart technologies and their societal impacts, this paper employs a qualitative, policy-oriented and interdisciplinary approach. It focuses on interpreting current trends and challenges rather than measuring them, drawing on relevant academic literature and policy documents to derive implications for defence policy.

2. The Social Dimension of Modern Technologies

The social dimension of modern technologies is reflected in digital society and its vulnerabilities, as well as in the role of social media and the broader information ecosystem. These interconnected domains highlight how technological advancement reshapes social structures, patterns of communication, and the distribution of information, influencing how individuals form opinions, interact within communities, and engage with public discourse. At the same time, they alter power dynamics between institutions, media actors, and citizens, redefining the ways in which information is created, disseminated, and consumed in contemporary society.

2.1. Digital Society and Vulnerability

The increasing dependence on digital technologies creates new societal vulnerabilities that extend far beyond the technical domain and directly affect the functioning of the state and the everyday life of citizens [11]. These include, for example, reliance on online services, exposure to cyber manipulation, and reduced resilience to disruptions.

The growing reliance on online services means that essential aspects of daily life (banking, healthcare, communication, public administration, access to basic utilities) are mediated through digital platforms. Societies that are highly digitized may be more efficient, but also more fragile. While this increases efficiency and accessibility, it also creates single points of failure. A disruption in digital infrastructure, whether caused by a cyberattack or technical malfunction, can quickly paralyze multiple sectors simultaneously. For example, the unavailability of online banking systems or e-government services can significantly disrupt economic activity and public administration.

Increased exposure to cyber manipulation represents a major societal risk. Individuals are constantly interacting with digital content, often without the ability to verify its credibility. This creates fertile ground for disinformation, propaganda, and psychological operations. Modern technologies, particularly social media algorithms and AI-generated content such as deepfakes, enable highly targeted and convincing manipulation (see e.g. [12-14]). As a result, public opinion can be influenced, trust in institutions weakened, and social divisions deepened (potentially without the population being aware of such interference).

Digital dependence reduces societal resilience to disruptions. In highly digitized societies, people gradually lose the ability to function without digital tools. Moreover the overuse of digital technologies has serious impact on cognitive mental processes [15]. Navigation, communication, financial transactions, and even critical thinking processes are increasingly outsourced to technology. In the event of a large-scale outage (cyberattacks, natural disasters, geopolitical conflict...) this dependency can lead to confusion, panic, and a slower recovery. Unlike traditional systems, digital infrastructures are often interconnected, meaning that failure in one sector can cascade into others.

Consequently, while digitalization enhances efficiency, speed, and connectivity, it simultaneously introduces systemic fragility. Highly digitized societies may therefore be more vulnerable to both intentional attacks and unintended disruptions. This paradox represents one of the key challenges for contemporary national defence and requires a balanced approach between technological advancement and resilience-building measures.

2.2. Social Media and Information Ecosystem

Platforms such as Facebook, X (Twitter), or YouTube have become central arenas for the dissemination of information, shaping public opinion, and enabling political influence and psychological operations [16–18]. Their algorithm-driven architectures prioritize engagement, often amplifying emotionally charged or controversial content, which can unintentionally contribute to the rapid spread of misleading or polarizing narratives. These platforms allow governments, organizations, and civil society to communicate quickly and directly with large audiences, increasing transparency and citizen engagement, which can strengthen democratic processes [16]. They also facilitate real-time crisis communication, mobilization of communities, and broader participation in public discourse.

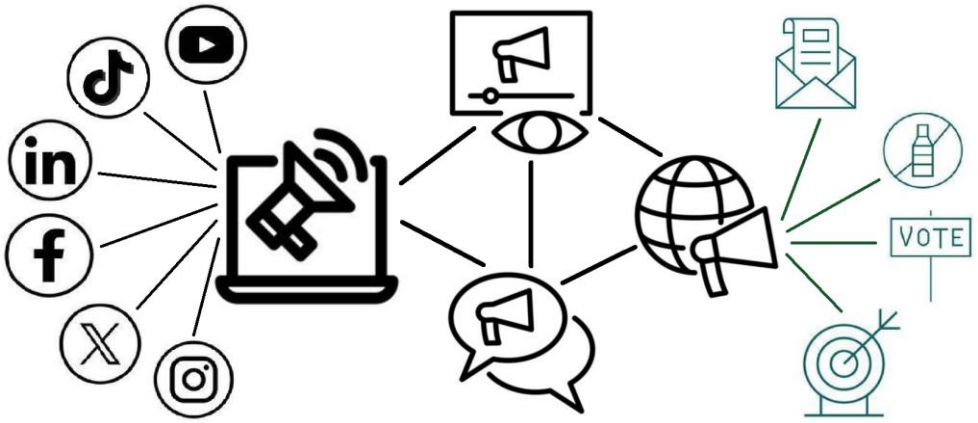

Fig. 1. The impact of social media.

At the same time, their widespread use makes them highly susceptible to exploitation. Malicious actors can spread disinformation, amplify polarizing content, and deploy AI-generated media, such as deepfakes, to manipulate perceptions and influence decision-making - see Fig. 1. In addition, coordinated inauthentic behaviour, bot networks, and microtargeting techniques enable adversaries to tailor messages to specific groups, increasing their persuasive impact while remaining difficult to detect. The speed, scale, and targeting capabilities of these platforms mean that misinformation can propagate faster than traditional corrective mechanisms, posing significant risks to social cohesion, public trust, and national security.

In this way, while social media and video platforms offer significant opportunities for empowerment, participation, and transparency, they simultaneously introduce systemic vulnerabilities. Addressing these challenges requires a combination of digital literacy, strategic communication, platform accountability, and adaptive regulatory frameworks. Ultimately, these platforms can both strengthen democratic governance and be exploited for manipulation, underscoring the need for a balanced and proactive approach to their role in contemporary security environments.

3. Key Technological Drivers

The key technological drivers within this context are: artificial intelligence (AI), big data and data analytics, internet of things (IoT), emerging technologies, and their convergence - see Fig. 2.

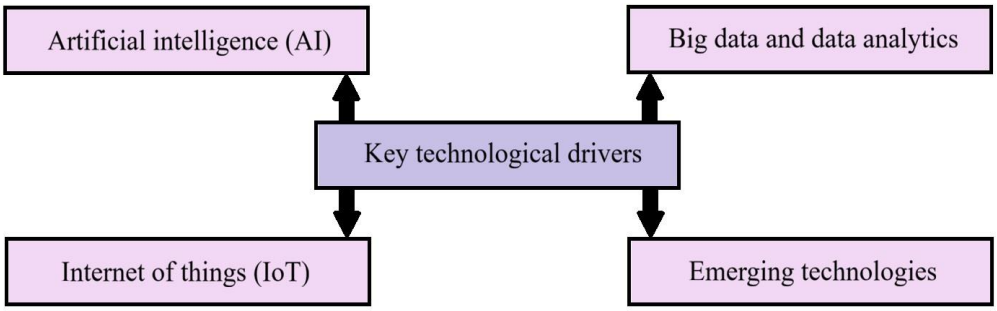

Fig. 2. Key technological drivers.

Artificial intelligence is transforming both civilian and defence sectors, enabling sophisticated surveillance, predictive analytics, and autonomous systems. In national security, AI can enhance threat detection, optimize decision-making, and improve the efficiency of military operations. However, its use raises critical concerns: biased algorithms may lead to unfair

outcomes, lack of transparency can undermine accountability, and autonomous systems may operate in ways that are difficult to predict or control (see [19-21]) Furthermore, AI can be exploited by adversaries to generate realistic fake content, automate cyberattacks, or manipulate public opinion, creating both strategic opportunities and vulnerabilities for states (see [22-25]).

The massive growth of data collection and processing capabilities allows governments and organizations to analyze complex patterns in society, economy, and security environments. Big data supports risk assessment, early warning of potential threats, and targeted decision-making in both defence and civil administration. However, the reliance on large-scale data analytics raises privacy concerns and legal challenges, as personal and sensitive information may be collected and processed without adequate safeguards. Misuse of data can erode public trust, making societies more vulnerable to manipulation and cyber exploitation.

The proliferation of connected devices - from smart homes and industrial systems to transportation networks and medical equipment, offers unprecedented efficiency and convenience. At the same time, IoT significantly expands the attack surface for cyber threats [26-27]. Vulnerabilities in even small or seemingly insignificant devices can be exploited to disrupt critical infrastructure, steal sensitive information, or propagate malware across networks. This interconnectedness, while beneficial for modern society, creates systemic risks that require comprehensive monitoring, regulation, and cybersecurity strategies.

Beyond AI, big data, and IoT, emerging technologies such as quantum computing, blockchain, and advanced robotics are increasingly relevant for national defence and societal functioning. These technologies often interact, creating complex systems that are difficult to secure and predict. The convergence of multiple technological innovations magnifies both capabilities and vulnerabilities, emphasizing the need for interdisciplinary approaches that integrate technical expertise, social sciences, and policy frameworks. States that fail to anticipate these interactions may face significant strategic disadvantages, while proactive integration can enhance resilience, deterrence, and societal security.

4. Social Challenges for National Defence

Modern technologies can both strengthen and undermine trust in public institutions. While digital platforms allow governments to communicate more directly and transparently with citizens, they also provide channels for disinformation, propaganda, and manipulative content. A society exposed to constant misinformation may experience declining confidence in its political and security institutions. This can weaken national cohesion and make coordinated responses to crises more difficult. For national defence, maintaining public trust is critical, as civilian support is essential for both policy implementation and resilience in times of conflict or cyberattacks.

Digital environments can amplify existing societal divisions, creating echo chambers [28] and filter bubbles where individuals are exposed only to information that reinforces their pre-existing beliefs [29]. This polarization can fragment public discourse and increase susceptibility to external influence, including foreign interference in elections or public debates. For national defence, a polarized society is more vulnerable to strategic manipulation, social unrest, and reduced collective resilience, making it harder to mobilize coordinated responses to threats or crises.

The human element remains one of the most significant vulnerabilities in national security. Cyberattacks, disinformation campaigns, or social engineering exploit human behaviors, such as trust, inattention, or lack of digital literacy. Even the most advanced technological defenses can fail if individuals unknowingly compromise systems or spread misinformation. Strengthening the human component through education, awareness programs, or training, is therefore essential to reinforce societal resilience and reduce exposure to manipulation or cyber exploitation.

The use of modern technologies in defence and security raises complex ethical and legal challenges. Governments must balance surveillance and data collection with respect for privacy, civil liberties, and democratic principles. Decisions about deploying AI in security contexts, regulating digital platforms, or countering disinformation require clear ethical guidelines and legal frameworks. Failure to address these issues can undermine legitimacy, provoke public backlash, and weaken the moral authority of national defence institutions.

Ultimately, modern social challenges highlight that national defence is not only about technology or military strength. It also depends on the resilience, awareness, and cohesion of society [30-31]. Building societal resilience involves integrating social sciences into security planning, educating citizens, fostering trust in institutions, and developing robust mechanisms to counter misinformation and polarization. A resilient society is better prepared to withstand both cyber and hybrid threats, making it a central pillar of contemporary national defence strategy.

5. Implications for Defence Policy

The contemporary social and technological challenges to national defence require a broader and more integrated approach to policy-making. As the boundaries between military, technological, and societal domains become increasingly blurred, defence strategies must reflect this complexity and interdependence. Key implications include:

- the need to integrate social sciences into security planning, ensuring that human behaviour, societal dynamics, and cultural factors are considered alongside technological and military capabilities;
- recognizing public perception and behaviour as a strategic factor, since the effectiveness of defence measures often depends on civilian understanding, trust, and cooperation;

- the development of societal resilience as a defence objective, strengthening the capacity of communities to withstand and recover from cyberattacks, disinformation, or other hybrid threats; and
- emphasizing the importance of strategic communication and counter-disinformation, ensuring that accurate information reaches the public and mitigates the impact of malicious manipulation.

Together, these measures highlight that effective national defence extends beyond technology and armed forces, encompassing societal preparedness, public engagement, and interdisciplinary policy design. Adapting to these challenges requires not only institutional innovation but also a sustained commitment to strengthening the relationship between the state, technology, and society.

6. Policy Recommendations Challenges

To address the complex social and technological challenges to national defence, key policy recommendations - see Fig. 3, can be summarized, as follows:

- Strengthen societal resilience through education and public awareness,
- Promote interdisciplinary approaches integrating social sciences with defence planning,
- Enhance international cooperation for collective security and cyber defence,
- Regulate and govern emerging technologies to ensure ethical and responsible use,
- Implement strategic communication and public engagement to counter disinformation and build trust.

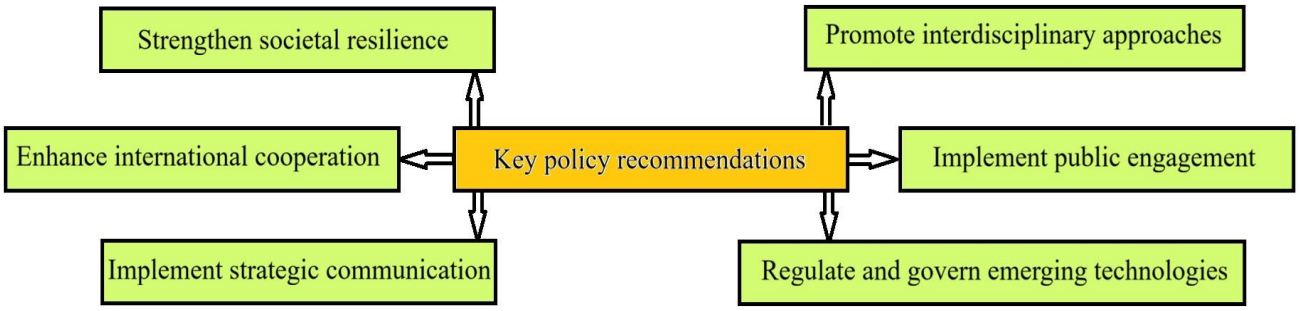

Fig. 3. Key policy recommendations.

A core recommendation for contemporary national defence is the enhancement of societal resilience. Governments and institutions should implement programs to improve digital literacy, public awareness of cyber threats, and emergency preparedness. Educating citizens about online misinformation, phishing, and social engineering tactics helps reduce vulnerabilities that adversaries can exploit. Resilient societies are better equipped to absorb shocks from cyberattacks, hybrid warfare, or infrastructural disruptions, minimizing both social and economic damage.

Addressing modern security challenges requires collaboration across multiple disciplines. National defence strategies should involve not only military and technical experts but also sociologists, psychologists, political scientists, and communication specialists. This interdisciplinary approach ensures that policies are informed by a deep understanding of societal behavior, cognitive biases, and communication patterns, allowing for more effective anticipation of threats and mitigation of risks in both cyberspace and the physical domain.

No nation can address contemporary threats in isolation. Policy recommendations emphasize strengthening cooperation at regional and global levels, including information sharing, joint cybersecurity exercises, and coordinated responses to hybrid threats. International frameworks, such as NATO's cyber defence initiatives and EU collaborative security programs, provide mechanisms for collective security, helping states counter state-sponsored cyberattacks, disinformation campaigns, and transnational cybercrime more effectively. Additionally, European data services and programmes, such as Copernicus, EU Satellite Centre (SatCen), and the European Union Agency for Cybersecurity (ENISA), offer critical support by providing real-time environmental, geospatial, and cybersecurity intelligence. These tools enhance situational awareness, early warning, and strategic decision-making, enabling member states to respond more efficiently to both physical and cyber threats, and to strengthen collective resilience across Europe.

As technologies such as AI, IoT, and big data become central to national defence and societal functioning, governments must develop clear regulatory frameworks to ensure responsible use. Policies should define ethical boundaries, accountability measures, and data protection standards, balancing security needs with civil liberties and democratic principles. Effective governance reduces the risk of misuse, strengthens public trust, and provides legal clarity in addressing technological threats.

Finally, effective policy must include proactive strategic communication and clear guidelines for the use of AI and data in security contexts to counter disinformation, manage public perception, and maintain trust in institutions. Transparent, consistent, and credible messaging helps citizens understand threats, respond appropriately during crises, and support national security measures. Engaging the public as a partner in resilience-building not only mitigates societal vulnerability but also reinforces the legitimacy and effectiveness of defence policies.

Conclusions

Modern technologies are not only tools of national defence but also forces that reshape society itself. Understanding their social impact is essential for addressing contemporary security challenges. Effective defence strategies must therefore combine technological innovation with deep insights from the social sciences.

Modern technologies are not only tools of national defence but also forces that fundamentally reshape society, influencing how security threats emerge, evolve, and are addressed. This paper has shown that the interaction between digital technologies and social dynamics creates a complex security environment in which vulnerabilities are no longer purely technical but deeply embedded in societal structures, behaviours, and perceptions. The increasing dependence on digital infrastructures, the influence of social media ecosystems, and the growing role of emerging technologies collectively redefine the conditions under which national defence operates.

The analysis highlights that technological advancement simultaneously enhances capabilities and generates new risks. While artificial intelligence, big data, and interconnected systems improve efficiency, situational awareness, and decision-making, they also expand the attack surface and amplify challenges such as disinformation, societal polarization, and erosion of trust. As a result, security threats increasingly exploit not only technical weaknesses but also cognitive and social vulnerabilities.

A key finding of this study is that effective national defence in the digital age requires a shift from purely state-centric and military approaches toward a more comprehensive model that integrates technological, social, and policy dimensions. Societal resilience, public trust, and strategic communication emerge as critical components of security, alongside technological capabilities. Without an informed, resilient, and cohesive society, even the most advanced defence systems remain insufficient.

Furthermore, the paper emphasizes the importance of governance and international cooperation. The transnational nature of cyber threats and technological risks necessitates coordinated responses, shared standards, and collaborative frameworks. At the same time, ethical and legal considerations must remain central to the deployment of emerging technologies, ensuring that security measures do not undermine democratic values and fundamental rights.

In conclusion, national defence in the digital era must be understood as a multidimensional and interdisciplinary endeavour. Future strategies should prioritize the integration of technological innovation with social awareness, education, and effective governance. Strengthening the link between technology, society, and policy will be essential for building resilient states capable of withstanding both current and emerging security challenges.

Acknowledgements. This work was supported in part by the Slovak Re search and Development Agency under the Contract no. APVV-22-0508 and no. APVV-18-0526, by the Slovak Grant Agency for Science under grant no. VEGA 1/0674/23, and the Cultural and Educational Grant Agency of the Ministry of Education, Research, Development and Youth of the Slovak Republic under grant no. KEGA 006TUKE-4/2024. This work was supported by the project Research on the elimination of engineering-geological barriers attacked by thermodynamic changes in simulated underground repository conditions using domestic mineral resources (X-rock), ITMS code: 401101B855, co-funded by the European Regional Development Fund.

References

1. **Montasari R.** Countering cyberterrorism: The confluence of artificial intelligence, cyber forensics and digital policing in US and UK national cybersecurity. Springer, Cham, 2023.
2. **Flor-Unda O., Puga D., Alomoto H. et al.** Evolution of technology for national security: Advances and contributions of artificial intelligence. Research Square, 2025. – Preprint.
3. **Sultan K., Madhi A.E., Mezher A.S., Al-Arar M.A., Anabtawi M.A.** Beyond traditional security: Leveraging emerging technologies for cyber resilience. Proceedings of IEEE EUROCON. Gdynia, 2025. p. 1–8.
4. **Botezatu U.-E.** Space technologies, smart cities, and national security: A smart(er) state synergy. Smart Cities International Conference (SCIC) Proceedings, 2024, p. 241–252.
5. **Jovanović A., Vollmer M.** Do. Smart technologies improve resilience of critical infrastructures. Critical Infrastructure Protection Review, 2017, 37, p. 1–10.
6. **Pînzariu A.-I.** Education as a smart power tool for national security. Editura Academiei Oamenilor de Știință din România.
7. **McCarthy D.R.** Imagining the security of innovation: Technological innovation, national security, and the American way of life. Critical Studies on Security, 2021, 9 (3), p. 196–211.
8. **Linkov I., Trump B.D., Poinsatte-Jones K., Florin M.-V.** Governance strategies for a sustainable digital world. Sustainability, 2018, 10 (2), p. 440.
9. **Milakovich M.E.** Digital governance: New technologies for improving public service and participation. Routledge, 2012.

10. **Marhasova V., Rudenko O., Popelo O., Kosach I., Sakun O., Klymenko T.** Mechanisms of state management of the development of digital technologies in the national security system. Revista de la Universidad del Zulia, 2024, 15 (42), p. 389–406.
11. **Fekete A., Rhyner J.** Sustainable digital transformation of disaster risk: Integrating new types of digital social vulnerability and interdependencies with critical infrastructure. Sustainability, 2020, 12 (22), p. 9324.
12. **Sophia L.I.** The social harms of AI-generated fake news: Addressing deepfake and AI political manipulation. Digital Society & Virtual Governance, 2025, 1 (1), p. 72–88.
13. **Mohammed A.** Deep fake detection and mitigation: Securing against AI-generated manipulation. Journal of Computational Innovation, 2024, 4 (1).
14. **George A.S., George A.H.** Deepfakes: The evolution of hyper-realistic media manipulation. Partners Universal Innovative Research Publication, 2023, 1 (2), p. 58–74.
15. **De Barros E.C.** Understanding the influence of digital technology on human cognitive functions: A narrative review. IBRO Neuroscience Reports, 2024, 17, p. 415–422.
16. **Boulianne S., Hoffmann C.P., Bossetta M.** Social media platforms for politics: A comparison of Facebook, Instagram, Twitter, YouTube, Reddit, Snapchat, and WhatsApp. New Media & Society, 2025, 27(11), p. 6006-6037.
17. **Kim S.J.** The role of social media news usage and platforms in civic and political engagement: Focusing on types of usage and platforms. Computers in Human Behavior, 2023, 138, 107475.
18. **Swastiningsih S., Aziz A., Dharta Y.** The role of social media in shaping public opinion: a comparative analysis of traditional vs. digital media platforms. The Journal of Academic Science, 2024, 1(6), p. 620-626.
19. **Kordzadeh N., Ghasemaghaei M.** Algorithmic bias: Review, synthesis, and future research directions. European Journal of Information Systems, 2022, 31 (3), p. 388–409.
20. **Mehrabi N., Naveed M., Morstatter F., Galstyan A.** Exacerbating algorithmic bias through fairness attacks. Proceedings of AAAI Conference on Artificial Intelligence, 2021, 35 (10), p. 8930–8938.
21. **Pagano T.P., Loureiro R.B., Lisboa F.V.N. et al.** Bias and unfairness in machine learning models: A systematic review on datasets, tools, fairness metrics, and identification and mitigation methods. Big Data and Cognitive Computing, 2023, 7 (1), p. 15.
22. **Arif A., Khan M.I., Khan A.R.A.** An overview of cyber threats generated by AI. International Journal of Multidisciplinary Sciences and Arts, 2024, 3 (4), p. 67–76.
23. **Blauth T.F., Gstrein O.J., Zwitter A.** Artificial intelligence crime: An overview of malicious use and abuse of AI. IEEE Access, 2022, 10, p. 77110–77122.
24. **Zdrojewski K.** AI-powered cyberattacks: A comprehensive review and analysis of emerging threats. Advances in IT and Electrical Engineering, 2025, 31, p. 55–70.
25. **Kharvi P.L.** Understanding the impact of AI-generated deepfakes on public opinion, political discourse, and personal security in social media. IEEE Security & Privacy, 2024, 22 (4), p. 115–122.
26. **Rizvi S., Orr R.J., Cox A., Ashokkumar P., Rizvi M.R.** Identifying the attack surface for IoT network. Internet of Things, 2020, 9, p. 100162.
27. **Stellios I., Kotzanikolaou P., Psarakis M., Alcaraz C., Lopez J.** A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Communications Surveys & Tutorials, 2018, 20 (4), p. 3453–3495.
28. **Rodrigues da Cunha Palmieri E.** Social media, echo chambers and contingency: A system theoretical approach about communication in the digital space. Kybernetes, 2024, 53 (8), p. 2593–2604.
29. **Spohr D.** Fake news and ideological polarization: Filter bubbles and selective exposure on social media. Business Information Review, 2017, 34 (3), p. 150–160.
30. **Fjäder C.** The nation-state, national security and resilience in the age of globalisation. Resilience, 2014, 2 (2), p. 114–129.
31. **Frey C.R.E.** Advances in technology and their impact on military resilience – response planning in the context of NATO's layered resilience concept. Proceedings of the 20th International Scientific Conference "Strategies XXI". 2024. p. 89–98.