

Internal security in the digital age – challenges and development areas

MICHAŁ ANTONIUK

Independent author



<https://orcid.org/0009-0006-7710-0685>

Abstract

The aim of this article is to present and systematise contemporary directions in the development of internal security in the context of advancing digital transformation. The subject of the study is the impact of digital technologies on the nature of internal threats and on the functioning of institutions responsible for ensuring state security. The article has a review-analytical character. The study employs a review of the relevant literature, an analysis of legal acts and strategic documents. The author compared the solutions for application of digital technologies in the field of security adopted in different countries and international organisations. The conducted analysis demonstrates that the development of these technologies has fundamentally transformed internal security systems, requiring changes in management models, the development of inter-institutional cooperation, and the adaptation of legal frameworks to emerging threats. In the conclusions, the author indicates that effective internal security in the digital age requires an integrated approach combining technological solutions, appropriate legal frameworks, development of institutional capacities, and international cooperation.

Keywords internal security, digital transformation, cybersecurity, digital threats, digital transformation

Introduction

Internal security constitutes one of the pillars of the state's functioning. It encompasses the protection of public order, the safety of citizens, critical infrastructure and stability of state institutions. Development of digital technologies brought about a fundamental change in the security environment. Contemporary threats are increasingly cross-border in nature, take place in cyberspace and have an impact on many aspects of the state's functioning at the same time¹.

The relevant literature emphasises that digitalisation not only enhances the effectiveness of functioning of the public administration and services responsible for security, but also creates new areas of vulnerability. The authors such as Barry Buzan, Myriam Dunn Cavelty or Richard Clarke and Robert Knake indicate that internal security now requires a shift away from a purely territorial view of threats towards an approach that takes into account cyberspace, critical infrastructure resilience and information security. In turn, data from the reports by the European Union Agency for Cybersecurity (ENISA) and the Organisation for Economic Co-operation and Development (OECD) indicate that the increasing number of cyber incidents forces the change in the way institutions responsible for security are organised and the development of public and private cooperation².

The research questions of this study are: how is the ongoing digitalisation affecting the functioning of the internal security system and what directions do contemporary scientific literature and strategic documents suggest for its development?

¹ B. Buzan, O. Wæver, J. de Wilde, *Security: A New Framework for Analysis*, London 1998, pp. 21–35; M.D. Cavelty, *Cyber-Security and Threat Politics. US efforts to secure the information age*, London–New York 2009, pp. 78–95.

² See for example: *ENISA Threat Landscape 2023*, European Union Agency for Cybersecurity, October 2023, <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf> [accessed: 11 VIII 2026]; OECD, *Digital Security and Resilience in Critical Infrastructure and Essential Services*, April 2019, https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/04/digital-security-and-resilience-in-critical-infrastructure-and-essential-services_5593c149/a7097901-en.pdf, pp. 34–37 [accessed: 11 VIII 2026].

The aim of the article is to systematise the current state of knowledge regarding the impact of digital transformation on the internal security and identification of the most important challenges, directions of development and solutions related to this, used in selected states and international organisations.

The article is of a review and analytical nature. An analysis of relevant literature, legal acts and strategic documents as well as the comparative method were used in the study. The application of these methods made it possible to collate the views presented in literature, to compare institutional and regulatory approaches and to formulate synthetic conclusions regarding the directions of development internal security in the digital age.

Transformation of the concept of internal security in the digital environment

Development of digital technologies brought about the fundamental change in the way the internal security is perceived. This concept previously associated primarily with the protection of public order, combating crime and ensuring the stability of the functioning of the state within its territory, has been extended to include the fight against cyber threats, which nature goes beyond the traditional approach to the state's security³.

Barry Buzan, Ole Wæver and Jaap de Wilde point out that security should be considered from the multidimensional perspective, encompassing not only military aspects, but also political, economic, social and technological. In their view, the development of information technology change the way the threats are identified and the state's response mechanisms, leading to an expansion of the scope of responsibility of the security institutions. This means that internal security should include not only protecting citizens against physical threats, but also ensuring resilience of digital infrastructure and security of information⁴.

Cavelty takes a similar view emphasising that digitalisation has led to the emergence of a new security environment in which threats are dynamic, difficult to predict and often cross-border. The author points out that cyberspace has become a sphere in which criminal activities, intelligence operations and disinformation campaigns can be carried out simultaneously against many countries, without the perpetrators needing to be physically present on their territory. As a result, traditional internal security instruments are insufficient unless supplemented by

³ B. Buzan, O. Wæver, J. de Wilde, *Security: A New Framework...*, pp. 27–29.

⁴ *Ibid.*, pp. 31–33.

organisational and technological solutions tailored to the specific characteristics of the digital environment⁵.

The ENISA also confirms the significance of this transformation. The organisation's 2023 report indicated that the number of attacks aimed at public administration, healthcare sector and critical infrastructure operators is steadily increasing. At the same time, the level of complexity of the methods employed is increasing, including, among others, ransomware attacks, phishing campaigns and activities conducted by state-sponsored groups. This means that internal security increasingly depends on the state's ability to protect digital infrastructure and respond rapidly to cyber incidents⁶.

A comparative analysis of the solutions adopted in selected states indicates that the process of adapting of the security institution proceeds at varying speeds. The EU Member States develop their systems primarily based on common legal regulations, such as the NIS2 Directive⁷ and cooperation within the ENISA.

In turn, the United States base their cybersecurity development on a risk management model, developed by the National Institute of Standards and Technology (NIST), in which the cooperation between public administration and private sector plays a special role⁸.

Both models aim to increase resilience of the state, however they differ in the scope of centralisation and the way of dividing responsibilities between public institutions and private entities.

A significant consequence of the digital transformation is also the change in the nature of the threats. Clarke and Knake indicate that cyber attacks may affect several sectors of the state simultaneously and lead to disruption of administration's work, financial systems, energy and transport. Nor do they require the use of military force or the physical presence of the perpetrator, and their consequences may include both economic losses, as well as social destabilisation and a loss of public confidence in public institutions⁹.

The relevant literature overview leads to a conclusion that internal security in the digital age should be viewed primarily as the state's capacity to ensure

⁵ M.D. Cavelty, *Cyber-Security and Threat Politics...*, pp. 78–81.

⁶ *ENISA Threat Landscape 2023...*, pp. 45–46.

⁷ *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).*

⁸ *The NIST Cybersecurity Framework (CSF) 2.0*, February 2024, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>, pp. 21–23 [accessed: 17 VIII 2026].

⁹ R.A. Clarke, R.K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, New York 2010, pp. 12–14.

the continuity of the functioning of its basic structures, protection of critical infrastructure and effective response to threats arising in cyberspace. This marks a shift away from a model focused on responding to incidents towards an approach based on building organisational resilience, risk management as well as national and international cooperation¹⁰.

Digital threats and their impact on the internal security

Development of digital technologies has led to a change in the nature of the threats affecting internal security of the state. Unlike threats that were local and physical in nature, digital threats are more often of a cross-border nature, are more difficult to identify, and their effects can affect multiple sectors of the state's functioning simultaneously. As David S. Wall notices, cybercrime is no longer a phenomenon limited to isolated cases of computer crime. It has become a complex system of criminal activity exploiting global information and communications networks. It encompasses both financial fraud, identity theft, and attacks on public administration, enterprises and critical infrastructure¹¹.

Clarke and Knake point out that cyber attacks are increasingly aimed not at individual IT systems, but at disrupting the functioning of entire economic and public administration sectors. Examples include ransomware attacks on hospitals, energy companies and local government administrative units, which result not only in data loss but also in temporary disruptions to public services. The authors emphasise that the effectiveness of such measures stems primarily from the high level of digitalisation of contemporary states and the interdependencies between ICT systems¹².

Disinformation campaigns that make use of social media and internet platforms constitute a separate category of threats. Lucas Kello points out that contemporary conflicts increasingly involve information campaigns aimed at influencing political processes and undermining public trust in public institutions and deepening social divisions. Unlike traditional attacks, these actions do not directly lead to the destruction of infrastructure but instead influence decision-

¹⁰ M.D. Cavelti, *Cyber-Security and Threat Politics...*, pp. 90–95; OECD, *Digital Security and Resilience...*, pp. 34–37.

¹¹ D.S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge 2007, pp. 55–57.

¹² R.A. Clarke, R.K. Knake, *Cyber War: The Next Threat...*, pp. 24–28.

making processes and public security, which makes them one of the most difficult challenges for the contemporary internal security systems¹³.

The significance of cyber threats are confirmed by the ENISA and OECD reports. They indicate that, since 2022, there has been an increase in the number of coordinated disinformation campaigns accompanying international conflicts and electoral processes. At the same time, it is pointed out that the effectiveness of measures to counter such threats depends on the technological solutions, the level of public education, citizens' information resilience and the efficient communication system of public institutions¹⁴.

A comparative analysis of the experiences of the European Union Member States and the United States points to different models of response to digital threats. In EU Member States, emphasis has been placed on the development of common security standards, incident reporting obligations and the protection of critical infrastructure arising from the NIS2 Directive. In the US, the basis is *the NIST Cybersecurity Framework (CSF) 2.0*. This is a risk management model that focuses on identifying threats, protecting assets, detecting incidents, responding to them and restoring operational capabilities after the attack.

The literature also draws attention to asymmetric nature of digital threats. Martin Libicki indicates that relatively small criminal groups or state-sponsored entities are capable of achieving effects comparable to conventional military operations exploiting vulnerabilities in ICT systems. This means that the effectiveness of actions depends not only on a state's economic and military potential but also on a level of its digital resilience, the preparedness of its public institutions and the quality of cooperation with critical infrastructure operators¹⁵.

The literature overview leads to a conclusion that digital threats include cybercrime, cyberterrorism, hybrid activities, disinformation operations and attacks on critical infrastructure, which all share the ability to simultaneously influence state's security, economy and society. For this reason, contemporary internal security should be regarded as a digital risk management system, which integrates technological, organisational and legal solutions, and not merely as actions taken after the occurrence of an incident¹⁶.

¹³ L. Kello, *The virtual weapon and international order*, New Haven–London 2017, pp. 59–62.

¹⁴ ENISA *Threat Landscape 2023...*, pp. 27–29; OECD, *Digital Security and Resilience...*, pp. 56–58.

¹⁵ M.C. Libicki, *Conquest in Cyberspace. National Security and Information Warfare*, Cambridge 2007, pp. 102–118.

¹⁶ D.S. Wall, *Cybercrime: The Transformation of Crime...*, pp. 55–70; S.W. Brenner, *Cybercrime and the Law: Challenges, Issues, and Outcomes*, Boston 2012, pp. 47–50.

The views presented in the literature also indicate that the effectiveness of protection against digital threats depends on the state's ability to anticipate new forms of risk and to continuously improve security procedures. In practice, this entails the need to regularly update national cybersecurity strategies, develop specialised competences within public administration, and deepen international cooperation regarding the exchange of information on threats and joint incident response. A comparative analysis of the experiences of the European states and the US confirms that actions based on prevention, building resilience and inter-institutional cooperation yield better results than a model that focuses on responding after an attack has occurred¹⁷.

Challenges relating to institutional adjustment and management

Progressing digitalisation necessitates a change in the way the institutions responsible for internal security operate. Traditional organisational models based on a hierarchical division of responsibilities and on reacting to incidents after they have occurred, prove to be insufficient in the face of threats characterised by high dynamism, cross-border nature and a high degree of complexity. The literature emphasises that the effectiveness of contemporary internal security system depends on the technologies available, but above all on the institutions' ability to adapt their organisation quickly, and to engage in effective cross-sectoral cooperation¹⁸.

Cavelty indicates that one of the most important problems of the contemporary security systems is a diffusion of responsibility for cybersecurity. In many countries, responsibilities relating to the protection of critical infrastructure, combating cybercrime, the protection of personal data and incident response are shared between government departments, special services, law enforcement and computer security incident response teams (CSIRT). Such a model increases the risk of duplication of tasks, which prolongs the decision-making process and hinders the efficient exchange of information¹⁹.

Similar conclusions were presented in the OECD report: *Digital Security and Resilience in Critical Infrastructure and Essential Services*. It points out that countries achieving the highest levels of digital resilience establish integrated security management systems in which the responsibilities of individual institutions are

¹⁷ OECD, *Digital Security and Resilience...*, pp. 34–37; *The NIST Cybersecurity Framework...*

¹⁸ M.D. Cavelty, *Cyber-Security and Threat Politics...*, pp. 78–82; OECD, *Digital Security and Resilience...*, pp. 39–42.

¹⁹ M.D. Cavelty, *Cyber-Security and Threat Politics...*, pp. 91–95.

clearly defined and cooperation between them is based on common procedures and regular exchange of information. The significance of strategic planning and continuous improvement of incident response procedures were also emphasised²⁰.

The comparative analysis carried out reveals clear differences between the digital security management models in the EU and the United States. In the EU Member States, the development of cybersecurity systems is primarily based on harmonising legislation, the cooperation carried out within the framework of the ENISA and the implementation of the NIS2 Directive. States were required to designate the competent authorities responsible for cybersecurity, establish national incident response teams and develop national digital security strategies²¹.

The US model is based on risk management and partnership between the public administration and private sector. The cybersecurity management framework developed by the NIST comprises five key stages: threat identification, assets protection, incident detection, response and restoration of operational capabilities. This solution is widely used by both the federal administration and enterprises managing critical infrastructure²².

An important element of the institutional transformation is the development of the skills of staff responsible for security. Henock Mulugeta Melaku points out that the effectiveness of the cybersecurity systems depends equally on the technologies used and on the level of specialist knowledge of the staff. In practice, this means that it is necessary to provide regular training, to develop skills in data analysis, digital forensics and security incident management. The shortage of highly qualified specialists is currently one of the most frequently cited constraints on the development of national cybersecurity systems²³.

Cooperation between public administration and private sector is also becoming increasingly important. A significant proportion of critical infrastructure, including energy, telecommunications, financial and transport systems, remains the property of private enterprises. Protecting these resources therefore requires the establishment of mechanisms enabling the ongoing exchange of information on threats, the conduct of joint exercises and the development of uniform response procedures. The experiences of Scandinavian countries and the Netherlands show

²⁰ OECD, *Digital Security and Resilience...*, pp. 55–57.

²¹ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity...

²² The NIST Cybersecurity Framework...

²³ H.M. Melaku, *A Dynamic and Adaptive Cybersecurity Governance Framework*, “Journal of Cybersecurity and Privacy” 2023, vol. 3, no. 3, pp. 347–350. <https://doi.org/10.3390/jcp3030017>.

that well-established public-private partnerships make it possible to identify threats more quickly and mitigate the effects of cyber incidents more effectively²⁴.

A review of the literature also indicates that institutional transformation must not be limited to the implementation of new technologies. It is equally important to foster an organisational culture that encourages cooperation, the sharing of knowledge and the continuous improvement of security procedures. Organisations characterised by a high degree of organisational flexibility adapt more effectively to a changing threat environment than institutions operating according to rigid, hierarchical management models²⁵.

In summary, it can be said that the development of internal security requires a comprehensive modernisation of public institutions. It encompasses investment in new technologies, reform of organisational structures, development of staff skills, establishment of sustainable mechanisms for cooperation with private sector, and the systematic improvement of risk management procedures. A comparative analysis of the experiences of EU Member States and the United States indicates that the greatest effectiveness is achieved by security systems that combine modern technological solutions with effective institutional management and a clearly defined division of responsibilities²⁶.

Legal and ethical aspects of internal security in the digital age

The digital transformation made it necessary to amend the existing legal regulations concerning internal security to threats in the cyberspace. The development of information technologies enabled public institutions to use tools based on big data analysis, the monitoring of ICT networks and the automation of decision-making processes. At the same time, the solutions sparked a debate on the limits of state interference in individual rights and freedoms. The relevant literature emphasises that effectiveness of measures taken in support of internal security should be consistent with the rule of law and standards for the protection of human rights²⁷.

²⁴ OECD, *Digital Security and Resilience* ..., pp. 51–53.

²⁵ Ibid.

²⁶ OECD, *Digital Security and Resilience*..., pp. 55–58; H.M. Melaku, *A Dynamic and Adaptive Cybersecurity Governance Framework*..., pp. 341–344; *The NIST Cybersecurity Framework*...

²⁷ *Constitution of the Republic of Poland of 2 April 1997*; *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*; M.D. Cavelti, *Cyber-Security and Threat Politics*...

The primary piece of legislation governing personal data protection in the EU Member States is *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* (hereinafter: the GDPR Regulation). This regulation establishes the principles of lawfulness, transparency, data minimisation and purpose limitation. From the perspective of internal security, this means that public authorities may use personal data only to the extent necessary to carry out their statutory duties and in accordance with the principle of proportionality. The GDPR Regulation does not restrict the ability to carry out activities relating to national security, but it does impose an obligation to ensure appropriate technical and organisational safeguards to protect the citizens' rights.

The second key element of the European legal system is the NIS2 Directive. Compared with the previous NIS1 Directive²⁸, the list of entities subject to obligations relating to cybersecurity has been expanded, and the requirements regarding risk management, incident reporting and the accountability of organisation's leadership have been tightened. These solutions reflect a shift in approach – from reacting to incidents to systematically building the resilience of states and critical infrastructure²⁹.

The *Convention of the Council of Europe on Cybercrime* known as the Budapest Convention³⁰ is also of significant importance for international cooperation. This document standardised the basic definitions of computer-related offences and established a framework for cooperation between law enforcement agencies in different states. As Susan Brenner points out, effectively combating cybercrime requires the harmonisation of legal regulations, as perpetrators often exploit differences between national legal systems. The Budapest Convention remains the primary instrument for international cooperation in the prosecution of offences committed using information technologies.

In Poland, the cybersecurity system is based on the Act on the national cybersecurity³¹ implementing the measures adopted at EU level. The act sets out the responsibilities of the public administration, operators of essential services and

²⁸ *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.*

²⁹ *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity...*

³⁰ *Convention of the Council of Europe on Cybercrime, done at Budapest 23 November 2001; S.W. Brenner, Cybercrime and the Law..., pp. 48–50.*

³¹ *Act of 5 July 2018 on the national cybersecurity.*

computer security incident response teams (CSIRT MON, CSIRT NASK and CSIRT GOV). Its aim is ensuring the efficient detection of incidents, the coordination of remedial actions and the exchange of information between institutions responsible for the state's security.

Regulations governing the use of artificial intelligence are also becoming increasingly important. The EU AI Act³² introduces a classification of artificial intelligencesystemsaccordingtotheirlevelofriskandsetsouttheobligationsofentities implementing solutions with a high level of social impact. In the context of internal security, this means it is necessary to ensure the transparency of the algorithms used, among other things, for analysing threats, monitoring public spaces and supporting the decision-making processes of the services responsible for security.

The legal aspects are closely linked to ethical issues. The development of monitoring and predictive analytics systems as well as artificial intelligence enhances the ability to prevent threats, but at the same time gives rise to the risk of infringing the right to privacy and of algorithmic discrimination. Cavelty emphasises that public acceptance of the use of modern technologies to ensure security depends on the transparency of procedures, the ability to monitor the activities of the administration, and effective appeal mechanisms. Citizens are more likely to accept a greater scope for state action if they are confident that such intervention is based on the law and is subject to independent oversight³³.

The comparative analysis indicates clear differences between the EU and the US approaches. Within the EU, priority is given to the protection of fundamental rights, privacy and the supervision of personal data processing. In the US, greater emphasis has been placed on the effectiveness of operational activities of the services responsible for the national security, while allowing a wider scope of powers to the institutions responsible for countering threats. These differences stem from differing legal and constitutional traditions. However, both models aim to strike a balance between the effectiveness of security measures and the protection of citizens' rights³⁴.

A review of the literature and applicable regulations lead to the conclusion that the development of internal security in the digital age requires the simultaneous improvement of legal instruments and ethical standards. Modern technologies

³² Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

³³ M.D. Cavelty, *Cyber-Security and Threat Politics...*, pp. 91–93.

³⁴ Ibid., pp. 91–95.

can significantly enhance the effectiveness of institutions responsible for security; however, their use should be within the limits set by the principles of proportionality, legality and accountability. Only by striking a balance between safeguarding national security and respecting individual rights can we build lasting public trust and ensure the effectiveness of the internal security system³⁵.

Technology as a tool for internal security

The development of digital technologies has significantly changed the way tasks relating to internal security are carried out. Modern IT solutions no longer merely support operations of public institutions, but have become one of the key elements in planning, monitoring threats and responding to them. As Clarke and Knake emphasise, contemporary state's security is increasingly dependent on the ability to make effective use of information technology in both preventive and operational measures³⁶.

One of the most important areas of development remains the use of data analysis and artificial intelligence. Modern security systems process vast amounts of data from monitoring systems, ICT networks, administrative registers and open-source intelligence (OSINT). The use of machine learning algorithms enables the identification of unusual behaviour, the prediction of potential threats and the support of decision-making processes. Melaku points out that the solutions based on artificial intelligence improve the effectiveness of cybersecurity management, provided that they operate within a properly designed risk management system and are subject to constant expert oversight³⁷.

Technologies supporting critical infrastructure monitoring also play a significant role. Automatic threat detection systems enable the real-time analysis of the operation of energy, transport, telecommunications and financial networks. The *ENISA Threat Landscape 2023* report indicates that the rapid detection of anomalies significantly mitigates the impact of ransomware attacks and other incidents targeting the state's infrastructure. For this reason, increasing emphasis

³⁵ Constitution of the Republic of Poland of 2 April 1997; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons...; Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence...

³⁶ R.A. Clarke, R.K. Knake, *Cyber War: The Next Threat*..., pp. 12–28.

³⁷ H.M. Melaku, *A Dynamic and Adaptive Cybersecurity Governance Framework*..., pp. 348–350.

is being placed on the development of early-warning systems and the automation of response procedures³⁸.

An example of the practical application of technologies are national and sectoral security operations centres, whose role is to monitor ICT networks around the clock and analyse any emerging threats. The operation of such units makes it possible to reduce the time taken to detect incidents and to coordinate remedial action more quickly.

The European Union and the United States have different approaches to the use of technology. The EU states simultaneously develop technology and regulatory system with a focus on personal data protection and critical infrastructure security. In the US, greater emphasis has been placed on cooperation between the federal administration and private sector as well as a development of innovative technologies devised by technology enterprises. The US model facilitates the rapid implementation of the new solutions, while the European approach provides stronger mechanisms for legal oversight of their application³⁹.

However, the increasing automation of security processes also brings new challenges. The public administration's growing reliance on IT systems means that a system failure or a successful cyberattack could lead to disruption across multiple sectors simultaneously. Libicki points out that increased digitalisation boosts both the efficiency of public institutions and the scale of the potential consequences of a security breach in IT systems. This means that solutions must be designed to ensure resilience, redundancy and the ability to quickly restore critical functions following an incident⁴⁰.

The literature also highlights the importance of cooperation between the scientific community, public administration and private sector. The rapid pace of technological development means that institutions responsible for security are unable to develop all innovative solutions on their own. The OECD indicates that partnerships involving universities, research institutes and technology companies facilitate the faster implementation of new analytical tools, improve the quality of risk management and increase the digital resilience of a state⁴¹.

A review of literature leads to the conclusion that technology is currently one of the most important means of ensuring internal security. However, its effectiveness depends on how it is integrated with organisational, legal and HR solutions.

³⁸ ENISA *Threat Landscape 2023*..., pp. 47–51.

³⁹ Ibid.; *The NIST Cybersecurity Framework*...; *Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons...*

⁴⁰ M.C. Libicki, *Conquest in Cyberspace*..., pp. 102–106.

⁴¹ OECD, *Digital Security and Resilience*..., pp. 34–39.

The mere implementation of new IT systems does not guarantee an increase in the level of security. It is of crucial importance to establish a coherent management model in which technological solutions support the decision-making process, while remaining subject to appropriate legal procedures and supervised by competent staff. An analysis of the experiences of the EU Member States and the United States confirms that the greatest effectiveness is achieved by systems that combine technological development with investment in human capital, inter-institutional cooperation and systematic risk assessment⁴².

The international context and a comparative perspective

Contemporary internal security cannot be analysed solely from the perspective of a single state. The development of digital technologies has meant that threats are increasingly cross-border in nature, and their effects extend beyond national jurisdictional boundaries. Cybercrime, disinformation campaigns and attacks on critical infrastructure are carried out using global ICT networks, which means that effective countermeasures require close international cooperation. As Kello points out, cyberspace has become a new arena for strategic competition, in which the boundaries between internal and external security are gradually becoming blurred⁴³.

Despite organisational differences, the European and American systems are based on similar strategic principles. In both cases, the following are of key importance: development of national cybersecurity strategies, building resilience in critical infrastructure, improving information-sharing systems and developing specialist expertise. The differences, however, lie in the way these objectives are achieved. In EU countries, greater emphasis has been placed on the harmonisation of legislation and the protection of fundamental rights, while in the US the focus has been on organisational flexibility and public-private partnerships⁴⁴.

The North Atlantic Treaty Organization (NATO) also plays a significant role in the international security system. Having recognised cyberspace as an operational domain, NATO is developing joint capabilities to counter cyber threats, conducting exercises involving Member States, and supporting

⁴² Ibid.; H.M. Melaku, *A Dynamic and Adaptive Cybersecurity Governance Framework...*, pp. 327–331; *The NIST Cybersecurity Framework...*

⁴³ L. Kello, *The virtual weapon and international order...*, pp. 45–62.

⁴⁴ OECD, *Digital Security and Resilience...*, pp. 34–58; ENISA *Threat Landscape 2023...*; *The NIST Cybersecurity Framework...*

the exchange of experience regarding the protection of critical infrastructure. These solutions increase the ability of states to respond to cross-border incidents and promote standardisation of security procedures⁴⁵.

The activities carried out by the United Nations and the Council of Europe are also becoming increasingly important. The Budapest Convention has laid the foundations for cooperation between law enforcement agencies in the fight against cybercrime, while the UN Expert Groups are drawing up recommendations on responsible state behaviour in cyberspace⁴⁶. Although these documents do not eliminate all differences between national legal systems, they contribute to the gradual harmonisation of international standards and facilitate cooperation in the prosecution of cybercrime offenders.

A comparative analysis of the documents leads to the conclusion that the effectiveness of internal security systems depends not on the adoption of a single, universal organisational model, but on the skilful adaptation of solutions to national circumstances, while drawing on international experience. A common feature of all the models analysed – that is, the EU and US models – remains the development of inter-institutional cooperation, building resilience in critical infrastructure, systematic exchange of information on risks and the continuous improvement of specialist skills. A review of the literature confirms that countries actively participating in international cooperation networks achieve a higher level of resilience to digital threats and respond more effectively to cross-border incidents⁴⁷.

Summary and conclusions

The analysis of the relevant literature, legal acts and strategic documents confirms that the ongoing digitalisation is leading to a fundamental change in the way internal security is perceived. Contemporary threats are less and less likely to be purely local or physical in nature, they are increasingly likely to spread to cyberspace, critical infrastructure and information environment. Consequently,

⁴⁵ A. Kozłowski, *Operacje NATO w cyberprzestrzeni* (Eng. NATO's operations in cyberspace), *CyberDefence*24, 3 VI 2019, https://cyberdefence24.pl/polityka-i-prawo/operacje-nato-w-cyberprzestrzeni#-goog_rewarded [accessed: 11 IX 2026].

⁴⁶ *Convention of the Council of Europe on Cybercrime...*; United Nations, *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135, 14 July 2021, pp. 57–59.

⁴⁷ OECD, *Digital Security and Resilience...*, pp. 51–54; ENISA *Threat Landscape 2023...*; *The NIST Cybersecurity Framework...*

internal security is to be understood as a system capable of identifying, mitigating and neutralising threats operating simultaneously in the technical, organisational, legal and social dimensions.

An analysis of the scholarly work of Barry Buzan, Myriam Dunn Cavelty, Richard Clarke, Robert Knake, Lucas Kello, David S. Wall and other researchers indicates that the development of digital technologies led to an expansion of the scope of liability of security institutions. Protection of public order now also includes ensuring the security of digital infrastructure, data protection, countering disinformation and building the public's resilience to information threats. This marks a shift away from a traditional security model focused on reacting after a threat has arisen towards a model based on risk management and building resilience.

A review of the literature also suggests that the effectiveness of the internal security system depends on the degree of integration of the activities carried out by the public administration, private sector and academic community. Protection of critical infrastructure, which in most countries remains largely owned by private entities, is of particular importance. Experiences in European countries and the United States show that well-developed public-private partnerships enable a more effective exchange of information on threats, a faster response to incidents and more effective risk management.

The EU states and the United States implement different models of digital security organisation. The European model focuses on harmonising legislation, protecting fundamental rights and building common cybersecurity standards. The US model places greater emphasis on risk management, organisational flexibility and cooperation between the administration and private sector.

An analysis of legislation indicates that the development of internal security requires the simultaneous improvement of regulations concerning the protection of personal data, cybersecurity and the use of artificial intelligence. The EU Regulation on the Protection of Personal Data, the NIS2 Directive, the Budapest Convention and the AI Act provide a complementary legal framework enabling measures to be taken to promote security while respecting civil rights and freedoms. This means that a balance must be struck between the effectiveness of the actions of security services and the protection of privacy, transparency in the administration's operations, and responsibility for the decisions taken.

On the basis of the analysis carried out, the following conclusions can be formulated:

1. Digitalisation has permanently changed the nature of internal security, extending its scope to include protection of the cyberspace, including systems supporting critical infrastructure and information security.

2. The greatest challenge for the contemporary security systems remains the ability of institutions to adapt their organisational structures and procedures rapidly to dynamically changing threat environment.
3. The effectiveness of internal security measures depends on cooperation of public administration, private sector and academic community, particularly in the field of protection of critical infrastructure and exchange of information on threats.
4. Modern technologies, including artificial intelligence, big data analysis and automation of security processes, enhance the capabilities of institutions responsible for security. However the use of these technologies requires appropriate legal and ethical safeguards.
5. Systems combining technological development and effective management, clear division of competences and extensive international cooperation achieve the highest effectiveness.

In the digital age, internal security requires an interdisciplinary approach, combining knowledge in the fields of security studies, law, management studies and information technology. Further development of the security systems will depend on the ability of states to implement innovative technological solutions while maintaining standards of the democratic state governed by the rule of law and the protection of human rights.

On the basis of the analysis carried out, the author also identifies areas for further research into the impact of artificial intelligence on the functioning of security institutions, an assessment of the effectiveness of the NIS2 Directive's implementation in the EU states, and a comparison of national models for building digital resilience. Knowledge on this subject can provide important recommendations for the practical operation of public administration and for further improvement of national internal security systems.

Bibliography

- Brenner S.W., *Cybercrime and the Law: Challenges, Issues, and Outcomes*, Boston 2012.
- Buzan B., Wæver O., Wilde J. de, *Security: A New Framework for Analysis*, London 1998.
- Cavelty M.D., *Cyber-Security and Threat Politics. US efforts to secure the information age*, London–New York 2009.
- Clarke R.A., Knake R.K., *Cyber War: The Next Threat to National Security and What to Do about It*, New York 2010.

Kello L., *The virtual weapon and international order*, New Haven–London 2017.

Libicki M.C., *Conquest in Cyberspace. National Security and Information Warfare*, Cambridge 2007.

Melaku H.M., *A Dynamic and Adaptive Cybersecurity Governance Framework*, “Journal of Cybersecurity and Privacy” 2023, vol. 3, no. 3, pp. 327–350. <https://doi.org/10.3390/jcp3030017>.

United Nations, *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135, 14 July 2021.

Wall D.S., *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge 2007.

Internet sources

ENISA *Threat Landscape 2023*, European Union Agency for Cybersecurity, October 2023, <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf> [accessed: 11 VIII 2026].

Kozłowski A., *Operacje NATO w cyberprzestrzeni* (Eng. NATO’s operations in cyberspace), CyberDefence24, 3 VI 2019, https://cyberdefence24.pl/polityka-i-prawo/operacje-nato-w-cyberprzestrzeni#goog_rewarded [accessed: 11 IX 2026].

OECD, *Digital Security and Resilience in Critical Infrastructure and Essential Services*, April 2019, https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/04/digital-security-and-resilience-in-critical-infrastructure-and-essential-services_5593c149/a7097901-en.pdf? [accessed: 11 VIII 2026].

The NIST Cybersecurity Framework (CSF) 2.0, February 2024, <https://nvlpubs.nist.gov/nist-pubs/CSWP/NIST.CSWP.29.pdf> [accessed: 17 VIII 2026].

Legal acts

Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws of 1997 no. 78, item 483, as amended).

Convention of the Council of Europe on Cybercrime, done at Budapest 23 November 2001 (Journal of Laws of 2015, item 728).

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) – (Official Journal of the EU L 333/80 of 27 XII 2022).

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union – (Official Journal of the EU L 194/1 of 19 VII 2016).

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) – (Official Journal of the EU L 2024/1689 of 12 VII 2024).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) – (Official Journal of the EU L 119/1 of 4 V 2016).

Act of 5 July 2018 on the national cybersecurity (Journal of Laws of 2018, item 1560, as amended).

Michał Antoniuk

He graduated from the University of Warsaw and completed postgraduate studies at the War Studies University. He is professionally involved in public administration and currently serves at the Ministry of National Defence, where he carries out tasks relating to security. His professional and academic interests include geopolitics and project management.

Contact: antonek@o2.pl

