https://www.sworldjournal.com/index.php/swj/article/view/swj31-01-083
DOI: 10.30888/2663-5712.2025-31-01-083

AI SOLUTIONS IN BUILDING NATIONAL CYBER MONITORING AND CRISIS INCIDENT MANAGEMENT SYSTEMS

Rudnytskyi Oleksii
ORCID: https://orcid.org/0009-0003-4062-941X
Owner, LLC "Standard Postachannya", Vostok Invest LLC

Abstract. *The article presents a systematic generalization and typology of artificial intelligence technologies applied not in the general context of cybersecurity but specifically for national cyber monitoring and crisis incident management. For the first time within a scientific analysis, a list of AI technologies is provided along with descriptions of their functional capabilities in the field of crisis response. The article outlines the key challenges of implementing AI in state security institutions and substantiates the need to develop a new generation of interdisciplinary specialists as a prerequisite for effective digital transformation of national security systems. The purpose of the article is to identify trends and justify the relevance of approaches for implementing artificial intelligence technologies in national cyber monitoring and crisis incident management systems. The research results show that national systems for cyber monitoring and crisis incident management are essential components of a state's cybersecurity architecture, as they ensure the ability to promptly detect, prevent, and respond to threats in the digital space. An analysis was conducted on the specific features of these systems, including the need for continuous monitoring of information flows, user behavior, network activity, and malicious impacts on critical infrastructure. It is proven that the evolution of digital threats has rendered traditional cybersecurity tools insufficient, prompting a transformation in security approaches and a shift toward advanced models based on big data analysis and predictive capabilities. The study demonstrates that modern AI-based solutions, including machine learning, deep learning, reinforcement learning, convolutional neural networks, and hybrid AI models, significantly enhance the efficiency of crisis response. These technologies enable behavioral analytics, detection of hidden cyber threats, real-time log analysis, and automated incident response. The integration of AI into cloud-based monitoring systems enables scalable data processing, minimizes human factor impact, and ensures rapid response. The practical significance of the study lies in establishing a methodological foundation for developing innovative AI solutions in the field of cybersecurity at the national system level.*

Keywords: *artificial intelligence, cyber monitoring, crisis incidents, national security, machine learning.*

Introduction

In the modern era of technological transformation, digitalization is penetrating every aspect of life – from everyday domestic needs to critical state institutions. At the same time, the development of artificial intelligence (AI) is advancing at an unprecedented pace: within just a few years, these technologies have evolved from experimental lab solutions to practical tools capable of real-time analytics, decision-making, process coordination, and nationwide automated management. This rapid progress brings large-scale challenges, with security emerging not merely as a relevant issue but as a defining one. Traditional approaches to protecting information systems

are proving inadequate in the face of increasingly complex cyber threats and the deep integration of digital services into public administration.

Security has long transcended individual, commercial, or even administrative concerns – it has become a systemic issue of national importance. Given that most key government functions – financial oversight, healthcare, energy, transportation, and defense – operate through digital platforms, any vulnerability in cyberspace potentially threatens national sovereignty. In this context, building an effective system for national cyber monitoring and crisis incident management using artificial intelligence technologies shifts from being a technical task to becoming a strategic priority that determines a state's ability to maintain integrity, stability, and resilience in the digital age.

The application of AI solutions for developing national systems of cybersecurity monitoring and incident management remains insufficiently explored in academic literature. Existing publications only partially address this topic, mostly focusing on related areas such as AI integration in cybersecurity, attack detection techniques, models of governmental cyber governance, or threat analytics. Nonetheless, several studies provide valuable theoretical and practical foundations for further analysis.

Among the most notable publications shaping the scientific background of this subject are those by authors who explore the role of AI in cybersecurity – L. Ofusori, T. Bokaba, S. Mhlongo [5]; M.K. Rahman, H. Dalim [6]; and C. Tiwari, S. Pillai, A.J. Obaid, A.R. Saear, A.K. Sabr [8]. Research on aspects of national cybersecurity governance is presented in the works of A. Davydiuk and O. Potii [2], as well as A. Santisteban, L. Ocares-Cunyarachi, and L. Andrade-Arenas [7]. Significant contributions to the development of cyber threat monitoring and detection methods have been made by N. Gupta, V. Jindal, and P. Bedi [3].

Despite the available literature, there is a clear lack of structured material on the subject of this study. Therefore, various scientific methods were applied to analyze, categorize, and organize the available information and present it in the context of the research topic.

Purpose of the article

The purpose of the article is to identify trends and justify the feasibility of applying approaches to the implementation of artificial intelligence technologies in national systems for cyber monitoring and crisis incident management.

Research results

Technology plays a profound role in addressing global threats. This issue concerns society as a whole and cannot be underestimated, especially considering the growing number of victims of cyberattacks targeting national information systems. Concerns about data fraud and cyberattacks have become critically important across the world. According to the General Packet Radio Service, a number of technological vulnerabilities have been identified: two-thirds of internet users are aware of the risks associated with identity theft, fake news, and data privacy, both in business and in the public sector [7].

Ensuring cybersecurity is an essential component of national security. The tasks involved in building a national system for cyber monitoring and crisis incident management include:

- active use of cyber tools in international competition;
- the competitive development of cybersecurity tools amid rapid and transformative changes in information and communication technologies, particularly in cloud and quantum computing, 5G networks, big data, the Internet of Things (IoT), artificial intelligence (AI), and others;
- the militarization of cyberspace and the development of cyberweapons, which enable covert cyberattacks to support military operations and intelligence or sabotage activities in cyberspace;
- the impact of global medical and military threats on economic activity and social behavior, which has led to a rapid transformation and reorganization of a significant segment of social relations into remote formats, heavily reliant on electronic services and automated control systems;
- the introduction of new technologies, digital services, and electronic interaction mechanisms between citizens and the state, which are being implemented

inconsistently within cybersecurity frameworks and often without proper risk assessment [2].

While information threats and risks may be universal in nature, national security strategies vary depending on the policies adopted by individual countries or regional alliances. For example, the European Union builds its strategies on the principles of data privacy protection, forming a context of ethical foundations and principles to safeguard the universal right to privacy [7]. Within the EU, a key role is played by the EU Cybersecurity Strategy for the Digital Decade (2020), which aims to build a resilient digital ecosystem capable of withstanding both internal and external cyber threats. A significant regulatory foundation is also provided by the Cybersecurity Act (Regulation (EU) 2019/881), which introduces a European cybersecurity certification framework and strengthens the mandate of the European Union Agency for Cybersecurity (ENISA). Additionally, the implementation of the NIS2 Directive (Directive (EU) 2022/2555) holds great importance, as it defines the responsibilities of member states in protecting critical infrastructure sectors, including energy, transport, healthcare, and finance.

In developed countries outside the EU – such as the United States, Canada, Japan, and South Korea – similar strategic documents have been adopted and tailored to the national context, including the National Cybersecurity Strategy (USA), Canada's National Cyber Security Strategy, the Cybersecurity Strategy of Japan, and the Korean National Cybersecurity Strategy. These frameworks emphasize coordination among state bodies, the development of cyber defense, collaboration with the private sector, enhancement of incident response capabilities, and international cooperation. In contrast, in Latin America, although most states have the capacity to respond to cyberattacks, only six have actually developed cybersecurity strategies. The latest country to introduce such a strategy was Mexico, which joined the small group of Latin American countries with similar policies – including Colombia, Panama, Paraguay, Chile, and Costa Rica – on November 13, 2017, according to data from the OAS [1].

As cyber threats have become more complex and sophisticated, cybersecurity has undergone a rapid evolution in recent years.

Table 1 – Evolution of technologies used in the development of national cybersecurity

Period	Technologies	Characteristics
Before 2000	Antivirus software, basic firewalls	Signature-based approach: antivirus programs, firewalls, manual threat database updates.
2000–2010	IDS/IPS, next-generation firewalls	Expanded tools, network-level protection, real-time updates.
2010–2015	SIEM, sandboxing, behavior analysis	Behavioral analysis, event correlation, automated detection of advanced attacks.
2015–2020	SOAR, threat intelligence, cloud security	Use of big data, automated response, expanded cloud-based solutions.
2020–present	AI/ML systems, Zero Trust Architecture, UEBA	Artificial intelligence, Zero Trust, behavioral biometrics, proactive defense.

Note: systematized by the author based on [6]

Traditional protection mechanisms based on signatures no longer provide an adequate level of resistance to modern cyberattacks. As noted by Rahman M.K. and Dalim H., conventional cybersecurity tools largely rely on predefined patterns to detect malicious activity, which makes them vulnerable to emerging attack vectors [6].

Modern security systems, in contrast, must be highly adaptive, polymorphic, and faster than human reaction capabilities [4]. Artificial intelligence in cybersecurity is increasingly viewed not merely as a tool for solving existing problems, but as a foundation for predictive analytics that supports a proactive approach to risk management. This approach enables not only a rapid response to incidents but also the anticipation of potential threats before they materialize.

The integration of predictive analytics into national cybersecurity strategies is gaining momentum due to its proactive nature. Implementing such models also helps reduce the number of false positives – a common issue for signature-based systems, which often misidentify benign activity as malicious. This is especially critical in high-risk environments, such as national cybersecurity infrastructures, where false alarms can lead to unnecessary resource expenditure. Moreover, the predictive capabilities of AI can be embedded into cyber intelligence systems, allowing the identification of emerging threats before they are executed. A study by Tomar S. and Singh P. demonstrated that AI-based cyber intelligence systems can process large volumes of unstructured data from various sources, including open sources, the dark web, and

historical attack data, in order to predict future cyberattacks. By identifying new threats and adversary tactics, these systems enable governments and organizations to proactively reduce risks and enhance the overall resilience of national cybersecurity [9].

Artificial intelligence in cybersecurity is almost never used as a standalone tool. Its effectiveness significantly increases when combined with other technologies that are either built upon its core algorithms or integrate its functionality into more complex systems. A summarized list of such technologies is presented in Table 2.

Table 2 – Technologies combined with AI in the field of cybersecurity

Technology	Application characteristics
Machine learning (ML)	Analysis of large data volumes, anomaly detection, adaptation to new threats.
Deep learning	Modeling complex dependencies, detection of APTs and other sophisticated attacks.
Reinforcement learning	Automated decision-making, adaptation based on feedback, reduced response time.
Convolutional neural networks (CNN)	Pattern recognition in network traffic and system logs.
Hybrid AI models	Combining learning methods to improve accuracy and resilience to emerging threats.
Cloud systems with AI integration	Real-time monitoring, scalability, reduced need for manual intervention.

Note: systematized by the author

AI-based systems use machine learning (ML) algorithms to analyze large volumes of data and identify behavioral patterns that may indicate potential security breaches. These systems are capable of detecting subtle changes in network traffic, user behavior, and system interactions that may go unnoticed by traditional monitoring tools [10]. As a subfield of AI, machine learning is particularly valuable in the context of national cyber monitoring and crisis incident management, as it enables systems to learn from historical data and adapt to new threats over time. For instance, supervised learning algorithms can be trained on labeled datasets containing both benign and malicious activity. Once trained, the system can use this knowledge to classify incoming events and assess their level of suspicion. Deep neural network models used to detect potential attack patterns through system log analysis have achieved accuracy rates of up to 92%.

This demonstrates AI's ability to recognize complex patterns in large datasets, allowing not only for reactive responses but also for predictive threat detection [6].

The role of machine learning in national cyber monitoring and incident management is further supported by a study conducted by Tiwari C., Pillai S., Obaid A.J., Saear A.R., and Sabr A.K., who proposed an automated incident response system using reinforcement learning. This approach allows national cyber monitoring systems to continuously adapt and optimize their actions based on outcomes of previous decisions. ML-based automation has been shown to reduce response time by up to 60% compared to manual methods. The authors also noted that reinforcement learning algorithms are especially effective in combating dynamic threats, as they can learn from both successful and unsuccessful actions, improving performance over time [8].

Similarly, other studies, including Gupta et al. (2019), have shown that AI-based IDS systems, particularly those utilizing convolutional neural networks (CNN), can automatically learn attack patterns from data and provide early warnings of network security breaches. These findings highlight AI's potential as a proactive, self-learning technology that continuously enhances its ability to detect and neutralize threats within national cyber monitoring and crisis response systems [3].

Deep learning – another subfield of AI – is a more advanced technique that uses multilayered neural networks to model complex relationships within data. Deep learning models have demonstrated high effectiveness in detecting advanced threats, including APTs (advanced persistent threats), malware, and other sophisticated incidents that can bypass traditional detection methods. Their ability to process and analyze large volumes of unstructured data, such as network traffic and system logs, makes them an optimal tool for protecting national infrastructure during crisis response scenarios.

The integration of artificial intelligence into cloud monitoring systems enables a powerful combination of scalability, real-time analysis, and adaptive learning. AI algorithms can continuously monitor an entire infrastructure, detecting and neutralizing threats as they arise. This approach reduces the need for human

intervention and allows national response teams to focus on more complex tasks, such as handling large-scale incidents and actively hunting threats [10].

Hybrid AI systems that combine various machine learning techniques are becoming increasingly popular in national cyber monitoring. For example, a system that combines supervised and unsupervised learning methods can improve the accuracy of threat detection in dynamic environments [5]. This combination enhances the generalization and resilience of models, making them particularly suitable for use in national crisis incident management systems.

Despite these advances, practical implementation of AI in national cyber monitoring still faces challenges, particularly with regard to data integration and real-time performance. In a study by Chirag Tiwari (2020), it was noted that integrating AI models with legacy systems in national security infrastructure is complex, as traditional cybersecurity protocols may be incompatible with AI-based tools. The integration process often involves overcoming barriers related to data isolation, technical system incompatibilities, and organizational inertia [8].

In addition, the use of AI in real-time requires high computational power and low latency, which places extra demands on resources in large-scale cyber operations. In their study, Ofusori, Lizzy; Bokaba, Tebogo; and Mhlongo, Siyabonga emphasized the need for high-performance computing (HPC) systems to effectively run AI models, particularly those requiring substantial data for training and inference. This challenge is further complicated by the need for real-time decision-making, where delays can lead to serious security breaches [5].

One of the key problems is the need for large volumes of labeled data to effectively train predictive models. In the context of national cyber monitoring and crisis response, acquiring high-quality labeled data is often hindered by privacy concerns, data fragmentation, and the constant evolution of threats [7].

Another major concern is the interpretability of AI models, especially those based on deep learning, which are often referred to as “black boxes.” The lack of transparency in decision-making complicates their use in critical areas where human oversight is required. To address this, recent studies have proposed the use of explainable AI (XAI),

which clarifies the decision-making process of the model, increasing its trustworthiness and practical value for professionals involved in national cyber monitoring and incident management. These approaches help bridge the gap between high-performance AI models and the need for transparency, allowing operators to make informed decisions based on insights provided by AI.

Based on the reviewed literature, the key challenges in implementing artificial intelligence in national cybersecurity systems can be summarized as follows (Table 3).

Table 3 – Key challenges in implementing artificial intelligence in national cybersecurity systems

Challenge	Explanation	Impact on security
False positives and false negatives	AI models may incorrectly identify safe activity as a threat or fail to detect actual threats.	Increased response time, risk of missed threats.
Integration with legacy systems	National infrastructure often relies on outdated systems that are incompatible with modern AI solutions.	Implementation becomes more complex and costly.
Data privacy and ethics	The use of AI may raise concerns about data collection and privacy violations.	Risk of personal data leaks and loss of public trust.
Complexity of AI model training	AI models require large and diverse datasets as well as continuous retraining.	High resource demand, risk of model obsolescence.
Allocation of resources for AI-based security	Implementing AI-based protection requires significant resource investment.	Budget constraints may hinder adoption, especially in smaller regions.
Scalability of AI models for large systems	AI models must be capable of processing large volumes of data.	System performance may decline as monitoring expands.
Human expertise for AI implementation and management	Skilled personnel are needed to deploy, monitor, and manage AI systems.	Shortage of experts may slow down implementation and usage of AI.

Note: systematized by the author based on [10]

Among the key challenges identified in the implementation of artificial intelligence in national cybersecurity systems, the issue of human resources stands out as particularly critical. The application of such technologies requires the involvement of highly qualified professionals who possess not only deep knowledge in programming and artificial intelligence but also an understanding of the functioning of

the national economy, critical infrastructure, and the interdisciplinary nature of public administration. This means that the next generation of cybersecurity specialists must have a broader range of competencies than those required in earlier stages of digital development.

Accordingly, the successful deployment of such systems must begin with the development of human capital – through education, retraining, and the fostering of professional communities. In countries with underdeveloped economies and weak educational infrastructure, sourcing such specialists may become a significant constraint. However, states that are already investing in educational programs, centers of excellence, and research initiatives in AI and cybersecurity will, in the long term, be better positioned to integrate effective, adaptive, and resilient protection systems capable of addressing modern threats. Given the projected rapid acceleration in the development of artificial intelligence technologies, the coming years will open new opportunities to strengthen the protection of government information systems, critical infrastructure, and digital sovereignty more broadly. This is why states must begin preparing for these challenges now by establishing the institutional, human, and scientific foundations necessary for future technological security [4].

Conclusions

National cyber monitoring and crisis incident management systems are integral components of the modern national security architecture, as they enable states to detect, prevent, and respond swiftly to incidents in the digital environment. A defining feature of these systems is the need for continuous monitoring of information flows, user behavior, network interactions, and potentially malicious activity within the infrastructure. Over the past decades, the concept of cybersecurity has evolved — from basic signature-based solutions (such as antivirus software and firewalls) to advanced predictive systems grounded in deep analysis of big data. This shift has been driven by the need to adapt to dynamic, high-tech threats increasingly targeting critical national assets.

The advancement of artificial intelligence (AI) technologies has significantly expanded the capabilities of crisis response. Modern solutions are built on machine

learning (ML), deep learning, reinforcement learning, convolutional neural networks (CNN), and hybrid AI models that combine various analytical and classification techniques. These technologies enable behavioral analytics, detection of hidden attack patterns, real-time system log analysis, and automated incident response. A particularly important aspect is the integration of AI into cloud monitoring systems, which ensures scalability, high-speed data processing, and reduced reliance on human intervention in the response process.

At the same time, despite these evident advantages, the effective implementation of AI in national cyber monitoring systems faces a number of challenges. The most pressing among them remains the shortage of specialists capable of developing, deploying, and maintaining AI-driven solutions in the field of cybersecurity.

References

1. Carr M. Public–private partnerships in national cybersecurity strategies. International Affairs, 2016, №92(1), 43–62. URL: https://doi.org/10.1111/1468-2346.12504

2. Davydiuk A., Potii O. National Cybersecurity Governance: Ukraine. Tallinn, 2024. National Cybersecurity Governance Series. URL: https://ccdcoe.org/uploads/2024/08/National-Cybersecurity-Governance_Ukraine_Davydiuk_Potii_2024.pdf

3. Gupta N., Jindal V., Bedi P. LIO-IDS: Handling class imbalance using LSTM and improved one-vs-one technique in intrusion detection system. Computer Networks, 2021, №192, 108076. URL: https://doi.org/10.1016/j.comnet.2021.108076

4. Kim Y.-J., Lee S.-Y., Kwon H.-Y., Lim J. A Study on the Improvement of Effectiveness in National Cyber Security Monitoring and Control Services. Journal of the Korea Institute of Information Security and Cryptology, 2009, №19. URL: https://www.researchgate.net/publication/264141653_A_Study_on_the_Improvement_of_Effectiveness_in_National_Cyber_Security_Monitoring_and_Control_Services

5. Ofusori L., Bokaba T., Mhlongo S. Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction. Applied Artificial Intelligence, 2024, №38. URL: https://doi.org/10.1080/08839514.2024.2439609

6. Rahman M.K., Dalim H. AI-Powered Solutions for Enhancing National Cybersecurity: Predictive Analytics and Threat Mitigation. 2023, №14, 1036–1069. URL: https://www.researchgate.net/publication/387269707_AI-Powered_Solutions_for_Enhancing_National_Cybersecurity_Predictive_Analytics_and_Threat_Mitigation

7. Santisteban A., Ocares-Cunyarachi L., Andrade-Arenas L. Analysis of National Cybersecurity Strategies. International Journal of Advanced Computer Science and Applications, 2020, №11. URL: https://dx.doi.org/10.14569/IJACSA.2020.0111288

8. Tiwari C., Pillai S., Obaid A.J., Saear A.R., Sabr A.K. Integration of artificial intelligence/machine learning in developing and defending web applications. AIP Conference Proceedings, 2021, №2736, 060038-1–060038-5. URL: https://doi.org/10.1063/5.0171097

9. Tomar S., Singh P. Cyber Security Methodologies and Attack Management. Journal of Management and Service Science (JMSS), 2021, №1, 1–8. URL: https://doi.org/10.54060/JMSS/001.01.002

10. Venkatesan K., Prasad M. Enhancing Cybersecurity for National Infrastructure Through AI-Powered Cloud Monitoring Systems. 2025. URL: https://www.researchgate.net/publication/388178026_Enhancing_Cybersecurity_for_National_Infrastructure_Through_AI-Powered_Cloud_Monitoring_Systems