**THE STRATEGIC ROLE OF AI IN ENHANCING NATIONAL CYBERSECURITY FRAMEWORKS**

**Abstract.** This study examines the key directions of artificial intelligence (AI) development and its influence on cyber defense strategies in national security. An analysis is conducted on current trends in the implementation of machine learning (ML) in cyberattack detection and prevention systems, demonstrating how AI technologies are transforming traditional approaches to forming National Cybersecurity Strategies (NCSS). The study identifies challenges and opportunities associated with the application of AI in protecting critical infrastructure, optimizing cyber incident management processes, and improving interagency coordination. Ethical considerations, legal regulation, and workforce development are discussed as critical aspects in the large-scale adoption of AI systems in government administration. Recommendations are proposed for enhancing NCSS through centralized management, adaptation of regulatory frameworks, strengthening public-private partnerships, and workforce capacity building. The study concludes by justifying the need for international cooperation, the development of global standards, and coordinated response mechanisms to cyber threats based on advanced AI solutions. This study demonstrates the critical role of artificial intelligence in transforming national cybersecurity strategies. By integrating advanced technologies with interdisciplinary approaches, AI not only enhances the detection and mitigation of threats but also facilitates the reform of traditional governance models amid ongoing digital transformation. The practical value of this work lies in its formulation of concrete recommendations aimed at harmonizing legal, ethical, and technical dimensions—thereby fostering a cohesive protection system for infrastructure through active collaboration among the state, private sector, and academic institutions. The findings will be useful for researchers and cybersecurity specialists, as well as government agencies responsible for shaping and implementing national cyber strategies.

**Keywords:** artificial intelligence, cybersecurity, national security, machine learning, National Cybersecurity Strategies (NCSS), public-private partnership, ethics and legal regulation.

**Introduction**

In the modern landscape, cyberspace has become a key domain for economic, political, and military interactions. The rapid growth of cyber threats, the increasing sophistication of attack methods, and the rising dependence of governmental structures on digital technologies drive researchers and practitioners to seek effective defense mechanisms. Artificial intelligence, particularly machine learning methods, is now regarded as one of the most promising areas capable of fundamentally transforming the cybersecurity landscape. At the national level, this implies not only the modernization of cyberattack detection and response tools but also a fundamental rethinking of digital risk management, including legal, organizational, and ethical dimensions.

A comprehensive review of contemporary research will be conducted. Kim G., Park K. [1] analyze the impact of artificial intelligence on the future development of national cyber defense strategies, emphasizing that their research aims to reconceptualize traditional approaches in response to the evolving dynamics of digital threats. Newman J. C. [3] formulates global aspirations toward creating a more resilient cybersecurity framework, establishing scientific novelty through an interdisciplinary analysis and synthesis of existing strategic models, while Lewis J. A. [4] proposes a rethinking of security concepts, hypothesizing that government structures can achieve a "mass effect" in combating cyber threats through the adaptation and modernization of strategic approaches. Methodologically, these studies rely on comparative analysis, forecasting, and the integration of theoretical models, highlighting a research gap in the insufficient adaptation of traditional security concepts to the realities of digital transformation.

A second body of research focuses on assessing threats associated with the malicious use of artificial intelligence. The work of Brundage M. et al. [2] is dedicated to forecasting, preventing, and mitigating the consequences of attacks, with the goal of developing comprehensive risk assessment models. The scientific novelty of this approach lies in identifying new cyberattack vectors arising from AI applications, while the authors hypothesize that timely detection and quantitative threat assessment can significantly reduce the likelihood of cyber incidents. The employed methods include analytical modeling, scenario analysis, and empirical validation, which help to define the existing gap in integrating preventive measures into national security strategy.

The third group of literature covers practical aspects of applying algorithmic methods for detecting and preventing cyber threats. Hussain H. et al. [5] demonstrate that their research aims to test machine learning technologies for rapid incident response, with scientific novelty manifesting in the development of hybrid models capable of adapting to evolving threats. Sarker I. H., Furhad M. H., Nowrozy R. [6] present a review of methodological approaches aimed at building intelligent security systems, hypothesizing that AI integration enhances anomaly prediction accuracy. Jimmy F. [7] focuses on identifying modern threats and defining the role of artificial intelligence in strengthening defense mechanisms, employing empirical and experimental methodologies to verify the effectiveness of developed systems. The methodological framework of these studies includes experimental modeling, big data analysis, and the application of intelligent analytics algorithms, revealing a gap in the systematic national-level testing of these solutions.

The fourth group encompasses publications offering comprehensive reviews and studies on contemporary applications of artificial intelligence in enhancing cybersecurity. Berman D. S. et al. [8], for instance, emphasize the use of deep learning methods for threat and anomaly detection, showcasing the potential of neural network approaches in automating cyber risk analysis. Reviews by Ofusori L., Bokaba T., and Mhlongo S. [9], along with the study by Haque M. M. and Rahman A. [10], cover a broad spectrum of AI algorithms—from traditional machine learning techniques to modern deep learning architectures—discussing their advantages, limitations, and development prospects in an increasingly dynamic cyber environment. In the context of forming integrated threat detection frameworks, Chowdhury M. J. M., Rahman M. S., Kayes A. S. M., et al. [12] present an analytical model that combines intelligent analytics with big data processing, enabling the development of adaptive response systems. Meanwhile, Achuthan K. et al. [13] highlight the necessity of aligning data protection strategies with AI methodologies, advocating for interdisciplinary approaches to address cybersecurity challenges.

The fifth group focuses on the application of advanced AI techniques within specific industries and infrastructure domains, which is becoming especially pertinent amid ongoing industrialization and digitalization. In particular, the study by Radanliev P. et al. [11] explores cyber risk analysis at the network edge, examining how predictive and analytical models can enhance system resilience in the Industrial Internet of Things and supply chains within the Industry 4.0 paradigm.

The sixth group centers on the strategic integration of AI technologies into national and digital security frameworks. The publication by Jonas D., Yusuf N. A., and Zahra A. R. [14] proposes conceptual models aimed at modernizing security systems through AI adoption, illustrating a cross-sectoral synthesis of technical and organizational solutions. In their study, Khan O. U. et al. [15] examine the application of AI for countering evolving threats and for constructing comprehensive digital defense mechanisms, emphasizing the importance of interagency and cross-industry collaboration.

Additionally, the review should consider a set of online resources chosen to provide statistical data on the role of artificial intelligence in bolstering national cybersecurity infrastructures. The following sources [16–20], whose findings are published on these websites, were consulted: PatentPC, VentureBeat, Infosecurity, JumpCloud, and WizCase.

The research gap lies in the fact that, despite extensive studies on AI-driven cybersecurity technologies, the question of how states should revise their national cyber strategies in light of AI implementation remains insufficiently explored. Most existing research focuses either on technical aspects (such as ML models and attack detection algorithms) or on a general understanding of the state's role, without systematically examining AI's impact on the core elements of National Cybersecurity Strategies (NCSS).

The objective of this study is to identify and analyze the impact of artificial intelligence on cyber defense strategies in national security, considering the expanded functions of NCSS.

The novelty of the research lies in examining not only the technical aspects but also the organizational, legal, and socio-ethical dimensions of AI integration into national cybersecurity strategies.

The study hypothesizes that AI adoption in cybersecurity affects the entire architecture of national cyber strategies by expanding its functionality (including critical infrastructure protection), increasing ethical and legal standards, and necessitating a new format of cooperation between the state and the private sector.

The methodological foundation is based on a comparative analysis of literature and statistical data on the impact of artificial intelligence on cyber defense strategies in national security.

**1. Contemporary trends in ai development in cybersecurity**

In the context of National Cybersecurity Strategies (NCSS), the integration of artificial intelligence, particularly machine learning methods, has undergone significant evolution in recent years. This transformation is reflected in the gradual expansion of technological solutions, the enhancement of proactive defense capabilities, and the increasing number of threats leveraging the same AI-driven tools.

The initial attempts to apply AI algorithms in cybersecurity date back to the early 2010s when specialists sought to automate network anomaly detection and malware identification using basic machine learning techniques. However, as noted by Kim and Park [1], these approaches were limited due to insufficient computational power and incomplete training datasets.

Since the mid-2010s, several factors have contributed to the advancement of AI in cybersecurity:

* The proliferation of big data, enabling the accumulation and processing of vast amounts of information on network traffic, vulnerabilities, and incidents [2].
* Accelerated progress in machine learning methods, including deep neural networks, reinforcement learning techniques, and time-series analysis for network behavior monitoring [6].
* The intensive commercialization of AI-driven cybersecurity solutions, with major IT companies offering automated threat detection and malicious traffic blocking systems [7].

Simultaneously, the threat landscape has evolved, with adversaries increasingly utilizing machine learning algorithms to bypass traditional attack detection mechanisms and refine intrusion strategies [9, 10]. As a result, governments face the necessity of not merely adopting AI-based cybersecurity tools but rethinking their defensive methodologies at a strategic level [1]. The primary applications of AI in cybersecurity are illustrated in Figure 1.

The main directions of using AI in cybersecurity

Automated detection of intrusions and vulnerabilities

User Behavior Analytics (UBA)

Security of critical infrastructure

Forecasting and proactive response

Automation of routine processes

Fig.1. The main directions of using AI in cybersecurity [1, 2, 5, 12].

Expanding on the key AI applications in cybersecurity depicted in Figure 1, the following areas warrant detailed analysis:

* Automated intrusion and vulnerability detection. Machine learning-based systems analyze logs and network packets in real-time to identify anomalies and suspicious patterns. This enables rapid response to attacks while reducing the burden on human analysts.
* User behavior analytics (UBA). To mitigate insider threats and account breaches, AI-driven systems monitor typical user activity patterns. Any deviations trigger alerts and prompt additional security checks.
* Protection of critical infrastructure. Industrial networks (SCADA/ICS), IoT devices, and cloud services increasingly rely on AI for early threat detection. Hybrid analysis models integrate data from physical sensors and network metrics to enhance security [13].
* Predictive analytics and proactive response. Machine learning enables the modeling of potential attack scenarios and their evolution. Decision-making is based on multidimensional analysis, factoring in vulnerability probabilities, attack pathways, and correlations with past incidents [8].
* Automation of routine processes. AI systems streamline tasks such as system monitoring, incident prioritization, and initial malware classification, allowing cybersecurity professionals to focus on complex challenges [1, 2, 5].

It is advisable to proceed with an analysis of the frameworks used to strengthen national cybersecurity systems. Framework-based standards such as the NIST Cybersecurity Framework, ISO/IEC 27001, and CIS Controls define maturity levels, assessment stages, and mechanisms for improving security processes. These structures enable government bodies to build strategic cybersecurity approaches based on widely recognized best practices and to respond rapidly to incidents.

Since 2012, ENISA has supported EU member states in developing and updating national strategies by providing implementation guidelines and conducting reviews of existing approaches.

In the United States, the NIST Cybersecurity Framework (CSF) is used on a voluntary basis but is institutionalized at the federal level through official reports and implementation methodologies. The updated CSF 2.0, published in February 2024, expands guidance on supply chain security and identity management, further solidifying the framework’s role as a regulatory baseline for contractor requirements across federal agencies [3, 14].

ISO/IEC 27001 remains one of the most influential international standards for establishing and advancing Information Security Management Systems (ISMS) at the national level. Governments apply this standard as a regulatory requirement for critical sectors such as banking, energy, and healthcare, thereby formalizing risk management processes and enabling ongoing monitoring of the effectiveness of protection measures.

The CIS Controls—a prioritized set of 18 practices designed to protect against the most common threats—are integrated into national strategies through NIST CSF recommendations and state-level legislative initiatives. Notable examples include the 2016 directive issued by the California Attorney General and the 2021 Colorado State Best Practices Guide. In parallel, ETSI has formalized the CIS Controls within its European technical specifications to ensure their regulatory applicability across the EU.

At the same time, ENISA, through the NIS Directive (2016) and its updated NIS2 Directive (2022), has developed the National Cybersecurity Assessment Framework. This framework is structured into four clusters—governance and standards, capacity building, legal and regulatory framework, and cooperation—providing member states with a comprehensive tool for assessing the maturity of national strategies and enhancing their ability to respond to cross-border incidents [7, 12].

When assessing the impact of artificial intelligence on national cybersecurity systems, research indicates that AI deployment can reduce the false-alarm rate by up to 90 % of all alerts without any loss of sensitivity [16]. This result was obtained via cross-validation on held-out event samples, ensuring high statistical reliability and minimizing overfitting risk.

In Security Operations Centers (SOCs), the “AI-copilot” concept cuts false-positive notifications by 70 %, which corresponds to a reduction in manual triage workload of over 40 analyst-hours per week [17].

The use of deep-learning algorithms—including recurrent and convolutional neural networks (RNNs, CNNs)—yields a 70 % increase in true-positive detection rates compared with classical heuristic methods [18].

Integrating streaming analytics with online-learning mechanisms delivers a 60 % improvement in the overall detection-efficiency metric, and average response times shrink from 168 hours to mere seconds in live infrastructure trials [19].

An AI model optimized for IoT devices achieves virus-detection accuracy of 98.53 %, opening new avenues for protecting critically important networks and assets [20].

The evolution of AI in cybersecurity is characterized by technological sophistication, shifting attack vectors, and expanded defensive capabilities within national security frameworks. However, successful implementation requires a systematic approach and a comprehensive assessment of associated risks. The next section will explore the impact of AI on transforming national cybersecurity strategies, detailing how AI advancements are reshaping their formulation and execution.

**2. Expanding the scope of NCSS**

Previously, national cybersecurity strategies primarily focused on technical aspects, including securing government networks, ensuring the resilience of critical infrastructure, and incident response. Figure 2 illustrates the potential applications of AI by the state.

The possibilities of using AI by the state

Monitoring and analysis of big data. Effective protection requires processing huge amounts of information in real time, from log files and telemetry to user behavioral characteristics. AI models allow us to rank threats by criticality and promptly initiate retaliatory measures.

Legal and ethical regulation. The introduction of machine learning (ML)-based systems addresses issues of privacy, the use of personal data, and the transparency of algorithms. Therefore, NCSS should contain provisions on respect for human rights and principles of openness when deploying AI solutions.

Supply chain management and development of internal AI competencies. The government has to rethink its dependence on global IT vendors, seek a balance between import and local development of AI products, and form a talent pool capable of maintaining and improving complex systems.

Fig.2. The possibilities of use by the state [1-3].

As highlighted by Lewis [4], public-private partnerships (PPP) serve as a cornerstone for developing advanced security solutions. In the context of AI, this is reflected in:

* Joint funding of R&D projects related to AI-driven monitoring and predictive analytics.
* Data sharing on incidents, standards, and best practices to enhance AI-based threat recognition models.
* Cross-licensing of technologies and the creation of test environments (sandboxing), where government agencies and private organizations can evaluate solutions before large-scale deployment [1, 3].

National cybersecurity strategies typically encompass multiple components that collectively define the priorities and strategic direction of a state's digital security efforts.

AI-driven systems facilitate proactive monitoring and network behavior analysis for critical infrastructure [1, 4]. This is especially crucial given the increasing frequency of complex, targeted cyber threats (Advanced Persistent Threats, APT) aimed at energy, transportation, and healthcare sectors.

AI-based intelligence systems collect and process vast amounts of personal data, increasing privacy risks. Consequently, NCSS should establish foundational principles to ensure data confidentiality, prevent algorithmic discrimination, and regulate AI abuse [3, 7].

The emergence of hostile AI systems capable of autonomously planning cyberattacks or even physical operations introduces a new phase of digital militarization [4].

The integration of AI into NCSS raises fundamental questions about prioritization in cybersecurity strategies. The following key areas are undergoing significant reassessment.

Traditional NCSS primarily focus on reactive measures (incident response). With the advent of AI technologies, predictive algorithms are gaining prominence, enabling:

* Real-time analysis of vast threat datasets to identify anomalies and generate scenario-based forecasts [6].
* Early-stage vulnerability detection during system design (DevSecOps practices utilizing ML models for code and component assessment) [11, 13].
* Prioritization based on the criticality of infrastructure and potential consequences [5, 7].

As emphasized by Lewis [4], private companies possess a significant share of the technological foundation and datasets essential for AI-driven cybersecurity advancements.

AI applications in cybersecurity are highly dependent on the quality and relevance of training datasets. Despite the clear advantages of AI tools, governments face several challenges in restructuring their cybersecurity strategies.

* Uneven levels of digital development across regions. Some areas lack basic internet infrastructure, hindering the implementation of advanced AI-based cybersecurity solutions.
* Shortage of interdisciplinary experts. The primary barrier to scaling AI projects in government administration is the lack of professionals skilled in both cybersecurity and algorithmic modeling.
* Ethical dilemmas. The collection of personal data for training ML models raises concerns over potential violations of citizens' rights. This has led to debates on the limits of government surveillance and the need for safeguards against unauthorized or excessive monitoring.
* The risk of an AI arms race and military AI deployment. Autonomous systems and AI-driven algorithms used in military operations (land, air, space, and cyber warfare) raise concerns over conflict escalation and the long-term consequences of AI militarization.

**3. Future development paths**

In the process of updating NCSS, it is essential to establish a clear hierarchy of responsibilities and authority. Practice demonstrates that the most effective approach involves the creation of centralized agencies. Given the rapid progress in ML, educational programs should be developed that integrate modules on mathematical statistics, neural networks, cyber threats, and legal aspects of security [6]. Collaboration with universities and research centers is crucial, as they can quickly incorporate emerging topics into curriculum.

AI in cybersecurity has a global dimension. To regulate the export of AI technologies and prevent an arms race, multilateral agreements are required, including those within the UN and other international platforms [3, 4].

Thus, under the influence of AI, national cybersecurity strategies are undergoing significant changes: objectives, priorities, and organizational structures within NCSS are evolving; new competencies and legal frameworks are emerging; public-private partnerships are strengthening, and the importance of international cooperation is increasing. A comprehensive approach enables governments to enhance defensive mechanisms while fostering a more resilient cyber environment in the long term.

The integration of artificial intelligence into national cybersecurity systems promises to significantly enhance proactive defense capabilities, yet it necessitates coordinated efforts from governments, businesses, and the academic community [1, 2].

The ongoing development of AI technologies in cybersecurity is a dynamic and multifaceted process, characterized by the increasing convergence of digital and physical security systems. Notably, there is a growing trend toward the creation of hybrid AI systems capable of operating across multiple domains, such as monitoring critical infrastructure and managing unmanned transport systems. Table 1 outlines future trends in AI development within the field of national cybersecurity.

Table 1. Trends in the development of AI in cyber defense for national security [1, 14, 15]

| **Development Path** | **Description** | **Challenges** | **Application in National Security** | **Recommendations** |
| --- | --- | --- | --- | --- |
| Integration of deep learning into threat detection systems | Utilizing neural networks and deep learning models to analyze large datasets and identify anomalies and hidden patterns in cyberspace. | Model interpretability, adaptation to new attack types, reduction of false positives, real-time data processing scalability. | Real-time monitoring of national infrastructure, automated detection of sophisticated and previously unknown threats. | Development of hybrid architectures combining deep learning with classical algorithms, research on explainable AI methods to improve trust in decisions. |
| Predicting cyberattacks using machine learning methods | Implementing predictive models and time-series analysis algorithms to assess the probability and nature of future cyberattacks. | Quality and completeness of training data, balancing false positives and false negatives, dynamic model updates based on evolving attack tactics. | Early warning of potential threats, optimizing resource allocation for countering attacks. | Research on multi-factor threat analysis, integrating statistical forecasting methods with modern ML algorithms, developing adaptive strategies based on obtained predictions. |
| Development of adaptive cyber defense systems using AI | Creating systems capable of self-adjustment and automatic response to attack vectors, ensuring continuous improvement of defense mechanisms. | Ensuring stability during autonomous algorithm changes, securing systems in the absence of constant human oversight, resilience to adaptation errors. | Automation of incident response processes, minimizing time required for threat localization and neutralization, enhancing the agility of critical infrastructure defense. | Applying reinforcement learning methods for training on real-world scenarios, developing self-diagnostic and self-correcting algorithms, conducting field trials with multidisciplinary teams. |
| Multi-layered behavior and anomaly analysis | A comprehensive approach combining analysis of user behavior, device activity, and network processes to detect anomalous activities across different layers of the information infrastructure. | Processing heterogeneous data, ensuring privacy in behavior analysis, detecting hidden and multi-stage threats amid high informational noise. | Monitoring user and device actions, detecting insider threats, overseeing critical national infrastructure objects. | Development of multi-agent analysis systems, combining statistical processing methods with AI algorithms, implementing data protection technologies in behavioral analysis. |

As part of the recommendations, the establishment of a specialized advisory body, similar to the AI Cybersecurity Council, is suggested. This body would not only develop recommendations for implementing advanced technologies but also ensure operational management, facilitating efficient resource distribution and accelerating decision-making processes.

A crucial requirement is the integration of legal norms into national laws and regulations to govern data collection, storage, and processing for training and testing AI models. Such an approach mitigates legal gaps, ensures transparent and responsible adoption of innovative technologies, and prevents potential misuse by both governmental and private entities.

The development of mechanisms for co-financing AI cybersecurity research, sharing real-time threat intelligence, and fostering cooperation in education forms the foundation for creating a synergistic effect. This combines cutting-edge private-sector technologies with the state’s ability to provide substantial financial resources and influence regulatory frameworks.

Finally, a key element of the national strategy involves systematic investment in human capital and the continuous development of education programs. The introduction of specialized AI and cybersecurity training programs in higher education institutions and professional development centers will ensure a steady supply of qualified specialists. These professionals will not only develop and implement cutting-edge AI solutions but also ensure their effective operation within government institutions. Strategic investments in educational initiatives contribute to the formation of an expert community prepared to address contemporary challenges and sustain the long-term development of national cybersecurity.

**Conclusion**

Based on an empirical analysis of statistical data, the pivotal role of artificial intelligence in strengthening national cybersecurity systems is confirmed. At the national level, this transformation necessitates an evolution of National Cybersecurity Strategies (NCSS), which must now account for a broad range of factors, including effective data management, legal frameworks, ethical standards, and the development of new professional competencies. The active implementation of AI-driven solutions for protecting critical infrastructure and managing cybersecurity processes requires comprehensive coordination across various government agencies, as well as close collaboration with the private sector, which possesses key technological expertise.

Particular emphasis is placed on balancing security interests with the protection of civil rights, along with the development of internationally recognized regulatory mechanisms that consider the specific applications of AI in military and intelligence operations. A major challenge remains the shortage of interdisciplinary specialists capable of working with machine learning methods while ensuring an adequate level of cybersecurity.

Based on the conducted research, it is evident that the findings can be practically applied to modernize national cybersecurity strategies through the integration of artificial intelligence systems into threat monitoring, analysis, and forecasting processes. Specifically, the use of hybrid models that combine deep learning with traditional algorithmic methods enables rapid anomaly detection, automation of routine tasks, and highly accurate prediction of potential cyberattacks. These approaches contribute to the protection of critical infrastructure by supporting the establishment of centralized cybersecurity operations centers and the development of interagency and public–private partnerships.

Furthermore, the results underscore the urgent need to adapt educational programs and enhance the professional training of specialists in both AI and cybersecurity. Such efforts form the foundation for a resilient model of national digital security. Implementing the proposed solutions enables the construction of a multi-layered defense system that not only anticipates cyberattacks but also responds swiftly to incidents already underway. This is achieved through hybrid deep learning models, automated anomaly detection, and adaptive self-correcting systems.

A comprehensive strategy that combines technological innovation with the development of institutional collaboration contributes not only to advancing threat detection capabilities but also to shaping an integrated legal and regulatory framework. This framework accounts for ethical concerns and data privacy, while facilitating dynamic coordination between governmental and private stakeholders. Additionally, the realization of these strategies requires long-term investment in human capital through the development of specialized training programs. This creates a sustainable knowledge base to support the ongoing evolution of national cybersecurity systems in the face of rapid digital transformation and an increasingly complex threat landscape.

The findings not only corroborate the study’s hypothesis—that integrating AI into cybersecurity transforms the entire architecture of national cyber strategies by expanding their functional capabilities (including critical‐infrastructure protection), elevating ethical and legal standards, and demanding a new model of public–private collaboration—but also underscore the imperative to further scale AI solutions within strategic national programs for safeguarding digital assets.

Nonetheless, the study is not without limitations, shaped by both methodological and empirical factors. First, the limited experimental validation of AI integration in real-world national infrastructure settings makes it difficult to assess the scalability and resilience of the proposed solutions—particularly under conditions of rapidly shifting threats. Second, the emphasis on interdisciplinary cooperation among technical, legal, and ethical domains remains largely conceptual and calls for further empirical investigation to evaluate the effectiveness of such integrated models in practice. These limitations highlight the need for continued work on refining algorithmic techniques, clarifying regulatory frameworks, and developing comprehensive approaches to workforce development that can facilitate synergy between public and private sectors.

Disclaimer (Artificial intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

**References**

1. Kim G., Park K. Effect of AI: The Future Landscape of National Cybersecurity Strategies //Tehnički glasnik. – 2024. – Vol. 18 (1). – pp. 29-36.
2. Brundage M. et al. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation //arXiv preprint arXiv:1802.07228. – 2018. – pp. 2-8.
3. Newman J. C. Toward AI security: global aspirations for a more resilient future //Center for long-term cybersecurity. – 2019. – pp.3-12.
4. Lewis J. A. Rethinking cybersecurity: strategy, mass effect, and states. – Rowman & Littlefield. - 2018. – pp.5-18.
5. Hussain H. et al. Leveraging AI and Machine Learning to Detect and Prevent Cyber Security Threats //Dialogue Social Science Review (DSSR). – 2025. – Vol. 3 (1). – pp. 881-895.
6. Sarker I. H., Furhad M. H., Nowrozy R. Ai-driven cybersecurity: an overview, security intelligence modeling and research directions //SN Computer Science. – 2021. – Vol. 2 (3). – pp. 173.
7. Jimmy F. Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses //Valley International Journal Digital Library. – 2021. – Vol. 1. – pp. 564-574.
8. Berman D. S. et al. A survey of deep learning methods for cyber security //Information. – 2019. – Vol. 10 (4). – pp. 122.
9. Ofusori L., Bokaba T., Mhlongo S. Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction //Applied Artificial Intelligence. – 2024. – Vol. 38 (1). – pp. 1-10.
10. Haque M. M., Rahman A.. Artificial Intelligence in Cybersecurity: A Comprehensive Survey // IEEE. - 2020. - Vol. 10. - pp. 26460-26490.
11. Radanliev P. et al. Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains //Cybersecurity. – 2020. – Vol. 3. – pp. 1-21.
12. Chowdhury M. J. M., Rahman M. S., Kayes A. S. M., et al. AI-empowered cyber threat intelligence and security solutions for next-generation networks: A comprehensive survey. // IEEE. - 2022. -Vol. 10. - pp. 20763–20794.
13. Achuthan K. et al. Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions //Frontiers in Big Data. – 2024. – Vol. 7. – pp. 1-10.
14. Jonas D., Yusuf N. A., Zahra A. R. A. Enhancing security frameworks with artificial intelligence in cybersecurity //International Transactions on Education Technology (ITEE). – 2023. – Vol. 2 (1). – pp. 83-91.
15. Khan O. U. et al. The Future of Cybersecurity: Leveraging Artificial Intelligence to Combat Evolving Threats and Enhance Digital Defense Strategies //Journal of Computational Analysis and Applications. – 2024. – Vol. 33 (8). – pp. 1-8.
16. AI and Cybersecurity: Latest Stats on AI-Driven Threat Detection and Attacks [Electronic resource] Access mode: <https://patentpc.com/blog/ai-and-cybersecurity-latest-stats-on-ai-driven-threat-detection-and-attacks?utm_source=> (date of request: 05/08/2025).
17. From alerts to autonomy: How leading SOCs use AI copilots to fight signal overload and staffing shortfalls [Electronic resource] Access mode: <https://venturebeat.com/security/ai-copilots-cut-false-positives-and-burnout-in-overworked-socs/?utm_source=> (date of request: 05/08/2025).
18. AI Boosts Malware Detection Rates by 70% [Electronic resource] Access mode:<https://www.infosecurity-magazine.com/news/ai-malware-detection-rates/?utm_source=> (date of request: 05/08/2025).
19. How Effective Is AI for Cybersecurity Teams? 2025 Statistics [Electronic resource] Access mode: <https://jumpcloud.com/blog/how-effective-is-ai-for-cybersecurity-teams?utm_source=> (date of request: 05/08/2025).
20. AI Model Achieves 98.53% Accuracy In Detecting Ransomware On Smart Devices [Electronic resource] Access mode:<https://www.wizcase.com/news/ai-model-achieves-98-53-accuracy-in-detecting-ransomware-on-smart-devices/?utm_source=> (date of request: 05/08/2025).