

**ARTIFICIAL INTELLIGENCE AND CYBERSECURITY
IN THE CONTEXT OF HYBRID THREATS: UKRAINIAN EXPERIENCE
AND REGULATORY APPROACHES**

Vitalii Andreichuk

*Candidate of Sciences in Public Administration,
Ukrainian Free University, Munich, Germany
Council for Information and Cybersecurity of Ukraine, Kyiv, Ukraine
<https://orcid.org/0000-0001-5238-5959>
Vitalii.Andreichuk@gmail.com*

Abstract

The article examines the relationship between the development of artificial intelligence (AI) technologies and current challenges in the field of cybersecurity in the context of hybrid warfare. Based on the experience of Ukraine, which has been in a constant state of information, cyber and military confrontation since 2014, the use of AI as a tool for both protection and potential threatening application is analyzed. Special attention is paid to the imperfection of the existing regulatory framework in the field of AI and cybersecurity, as well as proposals to create an integrated security system taking into account the latest technologies. The article offers conceptual and practical approaches to improving public policy, in particular through the introduction of ethical principles, interagency coordination and adaptation of international experience.

Keywords: Artificial intelligence, cybersecurity, hybrid threats, national security, Ukraine, regulation, ethics, digital sovereignty.

**ШТУЧНИЙ ІНТЕЛЕКТ ТА КІБЕРБЕЗПЕКА
В УМОВАХ ГІБРИДНИХ ЗАГРОЗ: УКРАЇНСЬКИЙ ДОСВІД
ТА РЕГУЛЯТОРНІ ПІДХОДИ**

Віталій Андрейчук

*Кандидат наук з державного управління,
Український Вільний Університет, Мюнхен, Німеччина
Рада інформаційної та кібербезпеки України, Київ, Україна*

Анотація

У статті досліджено взаємозв'язок між розвитком технологій штучного інтелекту (ШІ) та сучасними викликами у сфері кібербезпеки в умовах гібридної війни. Виходячи з досвіду України, яка з 2014 року перебуває у постійному стані інформаційного, кібернетичного та військового протистояння, проаналізовано використання ШІ як інструменту як захисту, так і застосування потенційних загроз. Особлива увага приділяється недосконалості існуючої нормативно-правової бази у сфері ШІ та кібербезпеки, а також пропозиціям щодо створення комплексної системи безпеки з урахуванням

новітніх технологій. У статті запропоновано концептуальні та практичні підходи до вдосконалення державної політики, зокрема шляхом впровадження етичних принципів, міжвідомчої координації та адаптації міжнародного досвіду.

Ключові слова: штучний інтелект, кібербезпека, гібридні загрози, національна безпека, Україна, регулювання, етика, цифровий суверенітет.

1. Introduction

1.1. Relevance of the topic in the context of war and digital transformation

The full-scale aggression of the Russian Federation against Ukraine has radically changed the perception of the role of digital technologies in national security. If earlier artificial intelligence (AI) and cyber tools were considered mainly as auxiliary means, today they have become critical elements of state defense¹. The war has demonstrated that traditional approaches to security have proven insufficient to counter modern hybrid threats, where information attacks are combined with cyber and physical impacts.

According to CERT-UA data, in 2024 the number of cyberattacks increased by nearly 70%, reaching 4,315 incidents compared to 2,541 in 2023². In the first half of 2025, 3,018 cyber incidents were recorded, representing a 17% increase compared to H2 2024³. Despite the growing number of attacks, the proportion of critical and high-level incidents decreased due to strengthening of cyber defense systems, demonstrating Ukraine's increasing cyber resilience.

In such conditions, the modern security doctrine is being reconsidered. Static protection systems are giving way to intelligent and algorithmic solutions capable of real risk analysis, autonomous threat intelligence and dynamic response to new challenges^{4,5}.

A landmark development in Ukraine's institutional response was the creation of Cyber Forces. On October 9, 2025, Ukraine's parliament approved Bill No. 12349 establishing the Cyber Forces as an independent command structure within the

¹ RAND Corporation. (2024). AI and National Security: Research Topics and Risks. <https://www.rand.org/topics/artificial-intelligence.html>

² CERT-UA. (2025). CERT-UA Recorded 4315 Cyber Incidents in 2024. State Service of Special Communications and Information Protection of Ukraine. <https://cip.gov.ua/en/news/cert-ua-minulogo-roku-opracuyvala-4315-kiberincidentiv>

³ CERT-UA. (2025). Russian Cyber Operations Analytics for H2 2024 [TLP:CLEAR]. State Service of Special Communications and Information Protection of Ukraine. <https://cip.gov.ua/services/cm/api/attachment/download?id=68768> Additional source: Dark Reading. (2025). Putin's Attacks on Ukraine Rise 70%, With Little Effect. <https://www.darkreading.com/threat-intelligence/putin-cyberattacks-ukraine-rise-little-effect>

⁴ Allen, G. C., & Husain, R. (2023). Artificial Intelligence and National Security. CNAS. <https://www.belfercenter.org/publication/artificial-intelligence-and-national-security>

⁵ Probasco, E., Toner, H., Burtell, M., & Rudner, T. G. J. (2025). AI for Military Decision-Making: Harnessing the Advantages and Avoiding the Risks. <https://cset.georgetown.edu/publication/ai-for-military-decision-making/>

Armed Forces of Ukraine⁶. This legislative initiative, supported by 255 lawmakers, formalizes Ukraine's offensive and defensive cyber capabilities under unified command, answering directly to the Commander-in-Chief.

1.2. Research objectives

The study is aimed at a comprehensive analysis of several interrelated aspects:

First, it is important to understand exactly how AI is changing the nature of cybersecurity in the context of hybrid warfare. Traditional threat models based on known attack patterns have proven insufficient against the enemy's adaptive algorithms⁷.

Secondly, it is necessary to analyze the features of legal, ethical and managerial support for the use of AI in the security sphere. The lack of clear norms creates risks of both insufficient protection and abuse by the defenders themselves⁸.

Third, it is critical to understand the dual nature of AI -- as a protection tool and a potential source of threats. The same technologies that protect critical infrastructure can be used to attack it⁹.

Finally, the study should suggest specific areas for improving national policy, taking into account both Ukrainian realities and international experience¹⁰.

1.3. Methodological basis

The study is based on a multidisciplinary approach that combines several methodological tools:

High-quality content analysis allows you to systematize and compare the approaches laid down in analytical documents, security strategies and legislation of Ukraine and NATO partner countries. Particular attention is paid to the evolution of these documents under the influence of the experience of hybrid warfare.

The systematic approach provides a comprehensive assessment of the technological potential of AI in the context of cyber defense. This allows you to identify not only individual capabilities of technologies, but also the systemic effects of their interaction.

⁶ Verkhovna Rada of Ukraine. (2025). Ukraine Parliament Approves Cyber Forces Legislation (Bill No. 12349, October 9, 2025). <https://www.rada.gov.ua/news/razom/266780.html>

⁷ National Institute of Standards and Technology. (2024). AI Risk Management Framework: Generative AI Profile (NIST AI 600-1). <https://doi.org/10.6028/NIST.AI.600-1>

⁸ Future of Life Institute. (2024). AI Policy -- National and International Governance. <https://futureoflife.org/ai-policy/>

⁹ Brundage, M., et al. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. arXiv. <https://arxiv.org/abs/1802.07228>

¹⁰ Danyk, Y., & Andreichuk, V. (2025). Artificial Intelligence in Countering Cyber Threats in Hybrid High-Tech Conflicts. [TACS 2025].

A comparative analysis of international practices of regulation and the use of AI in public security management provides an opportunity to adapt successful models to Ukrainian conditions.

The study of specific cases of the use of AI in the military field provides an empirical basis for theoretical generalizations and practical recommendations.

2. Conceptual foundations of the study

2.1. Artificial intelligence as a transformative security technology

AI in the field of national security represents a qualitatively new level of information processing and decision-making. Unlike traditional automated systems that perform pre-programmed functions, AI is able to adapt, learn, and generate new solutions in conditions of uncertainty¹¹.

Key technology areas include:

- **Deep learning** is the most revolutionary approach that allows systems to independently detect complex patterns in data without prior programming. As the researchers note: “Deep learning is a subset of machine learning that uses multi-level neural networks to detect complex patterns. Unlike traditional ML, DL is able to independently form features without manual intervention.”
- **Social media analysis** provides an opportunity to identify coordinated information campaigns, bots, and artificially created narratives in real time.
- **Deep analytics systems (Q&A systems)** provide rapid search and analysis of huge amounts of intelligence information.
- **Natural Language Generation (NLG)** and **virtual assistants** automate communication and processing of routine requests, freeing up human resources for more complex tasks.

Emerging AI threats in 2025: CERT-UA has documented the use of artificial intelligence by Russian hacker groups to generate malicious PowerShell scripts, marking a qualitative shift in cyber warfare tactics¹². The Wrecksteel malware, attributed to the UAC-0219 group, showed clear signs of AI-generated code. As CERT-UA warned: “The use of artificial intelligence in cyberattacks has reached a new level”¹³.

These tools allow you to implement fundamentally new capabilities: real-time threat assessment based on the analysis of millions of data sources, provide intelligent

¹¹ Danyk, Y., & Andreichuk, V. (2024). Artificial Intelligence in National Security and Defense: Opportunities and Challenges, Risk and Threat Mitigation. *Scientific collection of the Ukrainian Free University*, Vol. 25, 191-209.

¹² The Hacker News. (2025). CERT-UA Reports Cyberattacks Targeting Ukrainian State Systems with WRECKSTEEL Malware. <https://thehackernews.com/2025/04/cert-ua-reports-cyberattacks-targeting.html>

¹³ The Hacker News (2025), supra note 12

intelligence management with automatic prioritization, and use autonomous systems for rapid response to threats¹⁴.

2.2. Evolution of the understanding of cybersecurity

Cybersecurity has gone through a difficult path of evolution — from a highly technical discipline to a strategic element of national security. Today, it is a comprehensive system for ensuring the sustainability of the state's digital infrastructure.

Modern cybersecurity encompasses three critical dimensions:

- **The protection of critical infrastructure** includes not only technical aspects, but also organizational and legal mechanisms to ensure the continuity of the functioning of energy, transport, financial systems and public administration.
- **Countering cyber espionage and sabotage** requires an understanding of the motives and methods of state and non-state actors capable of complex long-term operations.
- **Monitoring the behavior of AI systems** is becoming a new critical task, as autonomous systems can exhibit unpredictable behavior or become targets of manipulation¹⁵.

Zero-click vulnerabilities as a new paradigm: In early 2025, CERT-UA recorded a significant surge in zero-click exploits — vulnerabilities allowing system infection without any user interaction¹⁶. Russian hackers exploited CVE-2023-43770 in Roundcube email platform, where malicious code executes merely by viewing an email. This represents a paradigm shift from social engineering to pure technical exploitation.

Three types of AI-related threats are especially dangerous in today's environment:

Uncontrolled actions of autonomous agents can lead to cascading failures in critical infrastructure. Harmful interference with the systems of the armed forces creates risks not only of a tactical, but also of a strategic nature. Data distortion through deepfake technologies and manipulative algorithms undermines trust in the information space as a whole¹⁷.

2.3. Hybrid threats as a new type of conflict

Hybrid warfare represents a fundamentally new type of conflict that blurs the traditional boundaries between peace and war, between state and non-state actors, between physical and virtual spaces. The Ukrainian experience since 2014

¹⁴ Allen & Husain (2023), *supra* note 4.

¹⁵ Future of Life Institute. (2024). Global AI Policy . <https://futureoflife.org/ai-policy/>

¹⁶ CERT-UA (2025), *supra* note 3.

¹⁷ ENISA. (2025). Threat Landscape Report 2025. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>

demonstrates that hybrid threats are not just a combination of different means of influence, but constitute a systemic strategy for destabilizing the enemy.

Key components of modern hybrid warfare include:

- **Traditional warfare** remains an important element, but its role and nature are changing dramatically due to integration with digital technologies.
- **Cyberattacks** are becoming not an auxiliary but an equal tool of influence capable of paralyzing the enemy's critical infrastructure.
- **Information influences** become systemic due to the use of AI to generate disinformation, create deepfakes, and conduct psychological operations.
- **AI tools in strategic communications** allow you to personalize propaganda messages and achieve maximum impact on target audiences.

Synchronized hybrid operations: Moscow continues to coordinate cyberattacks with missile and drone strikes to amplify disruptive effects, as documented by CERT-UA in their 2025 reports¹⁸. The Sandworm hacking unit, linked to Russia's GRU military intelligence, has been identified as orchestrating such synchronized hybrid attacks.

It is fundamentally important to understand that the hybrid threat is multidisciplinary and has no clear boundaries¹⁹. In this context, AI acts as both a protective barrier and a potential attack vector, making issues of standardization, ethical regulation, and legal support critical for national security²⁰.

3. AI and Cybersecurity: Synergy of Opportunities and Threats

3.1. Cyberspace as an arena for the application of artificial intelligence

Today's cyber environment is radically different from what existed even decades ago. If earlier cyber threats were mainly technical in nature and limited to relatively simple attacks, today we are dealing with complex, multi-level campaigns that combine technical, psychological, and social elements.

AI is transforming cyberspace in several key areas:

- **Automated threat detection** allows you to process amounts of data that are inaccessible to human analysis. Deep learning systems are capable of detecting anomalies in network traffic with an accuracy exceeding 90%, which is significantly superior to the capabilities of traditional methods²¹.

¹⁸ CERT-UA (2025), *supra* note 3.

¹⁹ Hoffman W., Kim H.M. (2023) Reducing the Risks of Artificial Intelligence for Military Decision Advantage. <https://cset.georgetown.edu/publication/reducing-the-risks-of-artificial-intelligence-for-military-decision-advantage/>

²⁰ European Commission. (2024). Regulation (EU) 2024/1689 on Artificial Intelligence (AI Act). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>

²¹ Cisco. (2024). Cybersecurity Readiness Index 2024. <https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m03/cybersecurity-readiness-index-2024.html>

- **Rapid classification and prioritization** ensure efficient allocation of limited security resources. AI can instantly identify the threat level and automatically initiate appropriate response procedures.
- **Adaptive learning** allows systems to continuously improve based on new experiences. Reinforcement learning technologies provide the ability to respond to previously unknown types of attacks.
- **Decision support** is especially important in crisis situations when reaction speed is critical. AI can provide operational recommendations and predictions of the development of the situation.

AI-powered defense in practice: According to Deputy Prime Minister Mykhailo Fedorov, Ukraine's government resources face approximately 100,000 cyberattacks monthly²². To counter this, the Ministry of Digital Transformation has deployed AI-based software on all employee laptops that monitors activity and responds instantly to unusual behavior, detecting threats that traditional antivirus programs miss.

However, this same technological power creates new vulnerabilities. AI systems are becoming attractive targets for so-called adversarial attacks — a deliberate modification of input data that is imperceptible to humans but forces the AI model to draw radically wrong conclusions²³. In a military context, this can lead to catastrophic consequences.

No less dangerous is the phenomenon of data poisoning — the deliberate introduction of malicious data into the sets on which the model is trained. This allows you to create hidden vulnerabilities that can be activated at a critical moment²⁴.

3.2. The Dual Nature of AI in the Context of Hybrid Threats

Hybrid threats require a rethinking of traditional approaches to security. If classical threats had clearly defined sources and methods, hybrid campaigns are characterized by multidimensionality, synchronization of various means of influence, and blurred authorship.

In this context, AI demonstrates its dual nature particularly vividly:

- **On the security side**, AI provides unique capabilities for detecting coordinated campaigns. Algorithms can analyze huge amounts of data from social networks, detecting artificially created botnets, deepfake content, and coordinated information operations.

²² United24. (2025). Ministry of Digital Transformation Cybersecurity Initiatives 2025. <https://united24media.com/latest-news/ukraine-faces-100000-cyberattacks-monthly-minister-of-digital-transformation-reveals-9231>

²³ Brundage, M., et al. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. arXiv. <https://arxiv.org/abs/1802.07228>

²⁴ Ferrara M. (2025). Data Poisoning and Artificial Intelligence Modeling: Theoretical Foundations and Defensive Strategies. https://ceur-ws.org/Vol-4031/04_regular.pdf

- **On the threat side**, the same technologies allow you to create highly sophisticated attacks. AI can generate personalized phishing messages, create compelling fake content, and automate the process of finding vulnerabilities in enemy systems.

The Ukrainian experience since 2014 demonstrates all aspects of this duality. On the one hand, Ukraine successfully uses AI to:

- Detection and analysis of Russian botnets in social networks
- Automatic recognition of disinformation and propaganda
- Monitoring of cyberattacks on critical infrastructure
- Analysis of satellite imagery to detect military activity

On the other hand, Russia is actively using AI to:

- Generation of sophisticated disinformation campaigns
- Creating deepfake content to discredit the Ukrainian leadership
- Automation of cyberattacks on energy infrastructure
- Personalization of propaganda messages

AI-guided malware emergence: CERT-UA researchers have identified malware that uses AI in real-time to determine next steps after network penetration²⁵. This represents a revolutionary tactical shift where malicious software adapts its behavior dynamically based on AI-generated recommendations, making traditional signature-based detection ineffective.

3.3. Practical application of AI in Ukrainian cyber defense

Ukraine has become a kind of testing ground for the most modern cyber defense technologies. The need to confront a powerful and technologically equipped enemy has accelerated the implementation of innovative solutions.

- **AI-based early warning systems** are already operating in energy and transport infrastructure. They are able to detect preparations for cyberattacks based on indirect signs and automatically initiate protective procedures.
- **Intelligent threat analysis** allows you to process information from tens of thousands of sources at the same time, identifying hidden connections and predicting probable scenarios.
- **Automated response systems** can instantly isolate infected network segments, redistribute loads, and activate backup systems without human intervention.
- **Collaboration platforms** combine data from different departments and private companies, creating a single picture of cyber threats on a national scale.

The Brave1 innovation ecosystem: Ukraine has created Brave1, a national defense tech cluster that has revolutionized defense innovation. As of 2025, Brave1 has:

²⁵ The Hacker News (2025), *supra* note 12

- Registered over 3,300 defense tech developments from more than 1,500 manufacturers
- Awarded over 540 grants totaling more than UAH 2.2 billion (approximately \$55 million), with an additional UAH 2.9 billion allocated in the 2025 national budget
- Facilitated over \$90 million in private investment since 2024²⁶
- Secured over \$100 million in pledged investments at the Defense Tech Valley 2025 summit in September, with participation of over 5,000 attendees from 50 countries, including €20M from NUNC Capital (Netherlands), €25M from Verne Capital (Germany-Luxembourg), and commitments from Swedish fund Varangians and Europe's first permanent defense-focused capital vehicle Oedipus Inc.²⁷

The Brave1 Defense Tech Innovations Forum in February 2025 brought together 3,000+ participants from 40 countries, showcasing Ukraine's emergence as a global defense tech hub²⁸. The initiative includes ethical oversight mechanisms and legal review of AI applications in military contexts, representing a model for responsible AI development in defense.

A particularly important achievement is the creation of specialized solutions for military use by Ukrainian developers. Artillery management system 'Kropyva' uses AI elements to process data from the battlefield, which significantly increases the efficiency of units.

3.4. System Challenges of AI Integration into Cyber Defense

Despite the obvious advantages, integrating AI into cyber defense systems faces several fundamental problems:

- **The problem of the "black box"** is that most modern AI systems cannot explain the logic of their decisions. In critical situations, this creates a risk of making wrong decisions without the possibility of correcting them.
- **Dependence on data quality** makes systems vulnerable to manipulation. Even small distortions in input data can lead to radically false conclusions.

²⁶ Brave1 Defense Tech Cluster. (2025). Official Statistics and Project Information. Ministry of Digital Transformation of Ukraine. <https://digitalstate.gov.ua/projects/tech/brave1> and <https://digitalstate.gov.ua/news/tech/brave1-market-ukrayina-zapuskaye-marketpleys-viyskovykh-innovatsiy>.

²⁷ Kyiv Post. (2025). Ukraine Secures Over \$100M in Defense Tech Investment at Brave1 Defense Tech Valley 2025. <https://www.kyivpost.com/post/60491>

²⁸ Brave1 Defense Tech Innovations Forum. (2025). Forum Results: 3,000+ Participants from 40 Countries (February 2025). Sources: DSEI. (2025). Feature: Ukraine's Brave1 Highlights Progress. <https://www.dsei.co.uk/news/feature-ukraines-brave1-highlights-progress-invites-collaboration> and United24 Media. (2025). Inside Brave1. <https://united24media.com/war-in-ukraine/inside-brave1-the-tech-hub-powering-ukraines-battlefield-innovations-7011>

- **The shortage of qualified personnel** is especially acute in Ukraine. The development and maintenance of AI systems for cyber defense requires a unique combination of competencies in the field of information technology, cybersecurity, and military affairs. Ukraine's cybersecurity market reached \$138 million in 2024 (a fourfold increase since 2016) but faces challenges in retaining talent against better-paid private sector opportunities²⁹.
- **Fragmentation of approaches** between different departments leads to duplication of efforts and inefficient use of resources.
- **Ethical dilemmas** arise when using AI to monitor its own citizens or make decisions that can affect people's lives.

Prompt injection attacks — a new frontier: Deputy Prime Minister Fedorov has warned about prompt attacks as an emerging threat to AI models³⁰. As Ukraine becomes the first government globally to face this challenge at scale with AI-integrated systems like Diia, the country is pioneering defenses against adversarial manipulation of large language models.

The issue of **digital sovereignty** is particularly complex. The development and training of advanced AI models require huge computing power and access to large, high-quality data sets.

4. Ukrainian experience: from theory to practice

4.1. Institutional architecture of cyber defense

The full-scale war with Russia has radically transformed the Ukrainian cybersecurity system. If before 2022 the institutional structure was formed evolutionarily, then the need to resist large-scale cyberattacks required revolutionary changes.

- **The National Security and Defense Council of Ukraine (NSDC)** has taken on the role of strategic coordinator. The Cybersecurity Strategy of Ukraine, adopted in 2021³¹, was the first document that recognized the need for the systematic use of AI for national security.

This strategic role is primarily executed through the key coordination body — **the National Cybersecurity Coordination Center (NCCC)**. The NCCC, which operates under the NSDC, ensures effective interagency interaction and operational monitoring of threats. It serves as the crucial platform where

²⁹ The Cyber Express. (2025). Ukraine's Cybersecurity Market Reached \$138 Million in 2024 (4x Growth Since 2016). Ukraine Reports 48% Jump In Cyber Incidents In H2 2024. <https://thecyberexpress.com/cyber-incidents-in-h2-2024-ukraine/>

³⁰ International Policy Digest. (2025). Deputy PM Fedorov Warns of Prompt Injection Attacks on Government AI Systems [Interview with Artem Moroz on AI Challenges]. Ukraine's Brave1 Is Racing to Redefine Warfare. <https://intpolicydigest.org/ukraine-s-brave1-is-racing-to-redefine-warfare/>

³¹ President of Ukraine. (2021). Decree No. 447/2021. On the Cybersecurity Strategy of Ukraine. <https://www.president.gov.ua/documents/4472021-40013>

decisions regarding the centralised deployment and ethical application of advanced AI technologies to enhance the resilience of critical infrastructure are made.

- **The Ministry of Digital Transformation of Ukraine** has turned from a department providing digital services into a key element of national defense. The Diia project has become not just an e-services platform, but a testing ground for the introduction of AI into public administration. User verification, fraud detection, and personal data protection systems use advanced machine learning algorithms.
- **The State Service of Special Communications and Information Protection of Ukraine (SSSCIP)**. As the central state authority for cyber defence and technical implementation, the SSSCIP is pivotal. It coordinates the core functions of CERT-UA and is responsible for the overall cyber protection policy of critical infrastructure, including government networks. The SSSCIP's role has been paramount in standardising advanced defensive cyber measures and implementing national threat intelligence sharing platforms to counter Russian aggression.
- **CERT-UA (Computer Emergency Response Team of Ukraine)**. Operating under the SSSCIP, CERT-UA transformed from a purely technical incident response service into a national-level analytical and prognostic center. The introduction of AI-based systems has allowed CERT-UA to shift from a purely reactive to a proactive model of operation, significantly enhancing its capability for predicting and preventing complex cyberattacks, particularly those targeting governmental bodies and critical infrastructure.
- **The Cyber Police** has become a pioneer in using AI to combat information threats. The developed systems automatically detect botnets, analyze deepfake content, and track the spread of disinformation on social networks.
- **The Security Service of Ukraine and the Armed Forces of Ukraine** have created specialized cyber defense units that use AI for reconnaissance activities, analysis of satellite images and coordination of hostilities.

Cyber Forces establishment: The creation of the Cyber Forces Command represents the most significant institutional development³². The Cyber Forces will:

- Organize, train, and equip cyber forces including a civilian cyber reserve
- Conduct offensive and defensive operations in cyberspace
- Report directly to Commander-in-Chief Oleksandr Syrskyi and President Zelenskyy
- Align Ukraine's cyber capabilities with NATO standards.

³² Verkhovna Rada of Ukraine. (2025). Ukraine Parliament Approves Cyber Forces Legislation (Bill No. 12349, October 9, 2025). <https://www.rada.gov.ua/news/razom/266780.html>

The Cyber Forces structure uniquely includes a civilian cyber reserve component, allowing motivated Ukrainian citizens with relevant skills to contribute to national cyber defense on a periodic basis without acquiring full military status. This innovative approach maximizes Ukraine's technological talent pool while maintaining operational flexibility.

4.2. Specific cases of AI application

The Ukrainian experience of using AI in cybersecurity is characterized by pragmatism and focus on real results:

- **The fight against disinformation** has become one of the most successful areas. The StopFake³³ and Detector Media³⁴ projects have integrated natural language processing (NLP) algorithms to automatically detect fake news. The systems analyze not only text content, but also metadata, distribution patterns, and user behavior. According to CERT-UA data, phishing remains the most common attack vector (27% of all incidents in H1 2025), with AI increasingly used to create convincing phishing messages³⁵.
- **Phishing protection** has reached a new level of effectiveness thanks to the use of deep learning. AI systems analyze email structure, writing style, technical characteristics, and contextual features, achieving detection accuracy exceeding 95%.
- **Analysis of the information space** allows you to track the spread of hostile narratives in real time. The systems detect coordinated information campaigns within hours after they start, which makes it possible to quickly organize refutations.
- **Satellite reconnaissance** using AI has become a critical tool. Computer vision algorithms automatically analyze images, detecting changes in the location of troops, the condition of infrastructure facilities, and signs of preparation for attacks.
- **Situational awareness systems** integrate data from dozens of sources — from technical sensors to social networks — creating a comprehensive picture of threats. Applications like Kropyva use this data to coordinate the actions of different units.
- **The cyber forces of the Armed Forces of Ukraine** use AI to analyze attack logs, identify enemy behavior patterns, and automate counterattacks. This allows effective countering of Russian hacker groups, despite their numerical superiority.

³³ StopFake. (2024). Fact-checking Ukraine. <https://www.stopfake.org/>

³⁴ Detector Media. (2024). Media Monitoring Ukraine. <https://detector.media/>

³⁵ Cyble. (2025). Government Sector Bears the Brunt of Cyberattacks in Ukraine: Report. <https://cyble.com/blog/ukraine-cyberthreat-landscape-2024/>

Malware analysis breakthroughs: CERT-UA's analysis of malware infections (21% of incidents in H1 2025) revealed sophisticated campaigns using legitimate cloud services like Dropbox, Google Drive, and Cloudflare for malware distribution³⁶. AI-powered detection systems have proven essential in identifying these campaigns that bypass traditional security measures.

4.3. Achievements and innovations

The Ukrainian experience has demonstrated several unique innovations that can be useful for other countries:

- **The integration of the public and private sectors** has reached an unprecedented level. Leading Ukrainian IT companies are actively cooperating with law enforcement agencies, providing technology and expertise. This model has proven to be much more effective than traditional public procurement. The Brave1 cluster exemplifies this approach, uniting manufacturers with military, government, investors and experts. In April 2025, Brave1 launched Brave1 Market — the first defense technology marketplace enabling Ukrainian military units to directly procure innovations using unit budgets and an innovative “combat points” system, where units earn points for verified target elimination that can be redeemed for needed technologies.³⁷
- **The speed of introduction** of new technologies has increased significantly. If in peacetime the implementation of a new system took years, then in wartime this process was reduced to several months or even weeks. The Brave1 Battle Proven competition accelerates this by fast-tracking technologies already deployed at the front³⁸.
- **The adaptability of the systems** has become a key advantage. Ukrainian developers have created AI systems that can quickly retrain when enemy tactics change. CERT-UA reports document how Russian hackers are forced to abandon outdated tactics and experiment with new AI-generated approaches as Ukrainian defenses strengthen³⁹.
- **Openness to innovations** made it possible to integrate the world's best practices with domestic developments. Cooperation with international partners provided access to advanced technologies and exchange of experience.

³⁶ The Cyber Express. (2025). Ukraine Reports 48% Jump in Cyber Incidents in H2 2024. <https://thecyberexpress.com/cyber-incidents-in-h2-2024-ukraine/>

³⁷ Brave1. (2025). Ukraine officially launches Brave1 Market — First online defense technology marketplace. Ministry of Digital Transformation. <https://digitalstate.gov.ua/news/tech/brave1-market-ukrayina-zapuskaye-marketpleys-viyskovykh-innovatsiy>

³⁸ Kyiv Post. (2025). Ukraine Secures Over \$100M in Defense Tech Investment at Brave1 Defense Tech Valley 2025. <https://www.kyivpost.com/post/60491>

³⁹ Kyiv Post (2025), supra note 27.

Ukraine's integration into the EU Cybersecurity Reserve in July 2025 enables rapid operational assistance from European teams during large-scale attacks⁴⁰.

4.4. System problems and limitations

Despite significant achievements, the Ukrainian experience has revealed several systemic problems that need to be urgently addressed:

- **The fragmentation of legal regulation** remains a critical challenge. The lack of a unified legislative framework for the use of AI in the security sector creates legal conflicts and slows down the adoption of new technologies. Law №4336, signed in 2025, establishes a unified NSDC-coordinated system for cyber incident response but gaps remain⁴¹.
- **The deficit of ethical standards** is especially acute when using AI to monitor citizens or make decisions that may affect their rights and freedoms. The lack of a generally accepted code of ethics creates risks of abuse.
- **Insufficient coordination between actors** leads to duplication of efforts and inefficient use of resources. Interaction between security agencies, IT companies and think tanks is often situational.
- **Dependence on foreign technologies** creates strategic risks. Most AI solutions are based on foreign platforms and computing power, which can limit autonomy in critical situations. Ukrainian customers prefer cybersecurity products from international companies, leaving local firms struggling to compete⁴².
- **Personnel shortages** remain one of the most pressing problems. Training specialists who can combine competencies in the field of AI, cybersecurity, and military affairs requires a long time and significant resources. The cybersecurity market is expected to reach \$208.80 million by 2029 with 8.54% annual growth, but talent retention challenges persist⁴³.
- **Corruption** in procurement and infrastructure protection represents a non-digital vulnerability that undermines technological defenses. Recent scandals, such as the 'Operation Midas' investigation in the energy sector (late 2025), highlight that AI-driven defense is ineffective if the physical and institutional foundations are compromised by malfeasance.

⁴⁰ Cyble (2025), *supra* note 35

⁴¹ The Cyber Express. (2025). Ukraine Reports 48% Jump In Cyber Incidents In H2 2024. <https://thecyberexpress.com/cyber-incidents-in-h2-2024-ukraine/>

⁴² Cyble (2025), *supra* note 35

⁴³ Statista. (2025). Cybersecurity — Ukraine. <https://www.statista.com/outlook/tmo/cybersecurity/ukraine>

5. Regulatory Framework: Challenges and Prospects

5.1. Global Context of AI Regulation

The global community is at the stage of forming new approaches to the regulation of artificial intelligence. Different countries and regions are choosing different strategies that reflect their values, priorities and level of technological development.

The European approach (AI Act) is characterized by an emphasis on the protection of human rights and ethical principles. The EU has adopted comprehensive legislation classifying AI systems according to risk levels — from minimal to unacceptable⁴⁴.

Especially important are the requirements for:

- Algorithm Transparency for High-Risk Systems
- Human oversight of critical decisions
- Regular audits and testing
- Personal Data Protection

The American model (NIST Framework) focuses on technical standards and industry self-regulation. The National Institute of Standards and Technology (NIST) has developed principles for the reliability, security, and accountability of AI, but has left significant leeway to the private sector⁴⁵.

Key elements of the American approach:

- Emphasis on innovation and competitiveness
- Minimal government intervention in technology development
- Prioritizing national security over privacy
- Active use of AI in the military sphere

NATO's strategy represents a compromise approach that combines democratic values with military necessity. In 2021, the Alliance adopted principles for the responsible use of AI in defense:

- Maintaining human control over critical decisions
- Reliability and predictability of systems
- Avoiding discrimination and bias
- Transparency and accountability⁴⁶

The OECD Principles for Responsible AI emphasize transparency, accountability, and inclusiveness. These principles have become the basis for the national strategies of many democratic countries⁴⁷.

⁴⁴ European Parliament and Council. (2024). Regulation (EU) 2024/1689 on Artificial Intelligence (AI Act). <https://artificialintelligenceact.eu/the-act/>

⁴⁵ National Institute of Standards and Technology. (2024). AI Risk Management Framework (NIST AI 600-1). <https://doi.org/10.6028/NIST.AI.600-1>

⁴⁶ NATO. (2023). Summary of NATO's Artificial Intelligence Strategy. https://www.nato.int/cps/en/natohq/official_texts_227237.htm

⁴⁷ OECD. (2019). OECD AI Principles. <https://oecd.ai/en/ai-principles>

At the same time, **the Chinese model** demonstrates a centralized approach with an emphasis on state control and social stability, which raises serious concerns about human rights and democratic values.

5.2. Ukrainian realities and legislative gaps

The national legislation of Ukraine so far covers the field of artificial intelligence only fragmentarily, which poses serious challenges to its safe and effective use.

Main legislative gaps:

- The lack of a basic law on artificial intelligence leaves uncertain the legal status of AI systems, responsibility for their actions, and security standards.
- Outdated norms in the field of information security do not take into account the specifics of algorithmic risks, working with big data, and the peculiarities of neural network technologies.
- The lack of ethical standards for the use of AI in public administration creates risks of violation of citizens' rights and abuse by officials.
- Inconsistency of departmental standards leads to legal conflicts and complicates interagency interaction.

Specifics of martial law:

- The need for quick decision-making in wartime requires simplification of procedures for the introduction of new technologies, which may contradict the principles of proper legal regulation.
- The use of AI in the military sphere requires a balance between effectiveness and compliance with international humanitarian law.
- The involvement of foreign technologies and expertise requires consideration of issues of national security and technological sovereignty.

Recent developments: The major breach of state registries at the turn of 2024-2025 accelerated adoption of Law №4336, which establishes mandatory cybersecurity officer positions at critical infrastructure facilities and strengthens the State Service of Special Communications and Information Protection⁴⁸.

5.3. Strategic recommendations for Ukraine

Taking into account international experience and its own needs, Ukraine should develop a comprehensive strategy for AI regulation that considers both the current challenges of the war and long-term development goals.

Adaptation of European standards should be a priority in the context of European integration. However, direct copying of the AI Act may not be effective due to differences in the legal system and current security needs.

⁴⁸ Verkhovna Rada of Ukraine. (2025). Law No. 4336 <https://zakon.rada.gov.ua/laws/show/4336-20#Text> For English summary see The Cyber Express (2025), *supra* note 29.

The development of a national law on artificial intelligence should cover:

- Classification of AI systems by risk level
- Certification and Audit Procedures
- Mechanisms of liability and compensation for damages
- Features of use under martial law
- Specific provisions for AI-generated malware detection
- Standards for zero-click vulnerability protection

The creation of an AI ethics council under the Cabinet of Ministers will allow for expert evaluation of projects and the development of industry standards. The Bravel model demonstrates how legal oversight and ethical review can be integrated into defense tech development⁴⁹.

Interagency coordination should be formalized through the creation of a permanent coordinating body with representatives of all interested agencies. The creation of Cyber Forces Command provides a foundation for this coordination⁵⁰.

International cooperation within the framework of the G7, NATO and the EU will allow us to use the best international practices and avoid isolation. Canada's allocation of 92 million UAH (\$2.2M USD) to strengthen Ukraine's cybersecurity systems exemplifies this cooperation⁵¹.

6. Ethical dilemmas and managerial challenges

6.1. Fundamental ethical issues

The use of artificial intelligence in the field of cybersecurity gives rise to a complex of ethical dilemmas that do not have simple answers. These issues become especially acute in wartime, when traditional ethical norms face the need to ensure the survival of the nation.

- **The problem of responsibility for autonomous decisions** is one of the most complex. When an AI system independently decides to block critical infrastructure, spread disinformation countermeasures, or identify an individual as a potential threat, the question arises: who is morally and legally responsible for the consequences?

The Ukrainian experience shows the complexity of this problem in practice. When an autonomous cyber defense system mistakenly blocked access to an important resource during a critical situation, the question arose: was the algorithm developer, the system operator, the commander who activated it, or the technology itself to blame?

⁴⁹ OECD. (2019). OECD AI Principles. <https://oecd.ai/en/ai-principles>

⁵⁰ Verkhovna Rada of Ukraine. (2025). Ukraine Parliament Approves Cyber Forces Legislation (Bill No. 12349, October 9, 2025). <https://www.rada.gov.ua/news/razom/266780.html>

⁵¹ Ukrinform. (2025). <https://www.ukrinform.net/rubric-society/4039965-canada-allocates-92-million-to-ukraine-to-strengthen-cybersecurity.html>

- **The balance between security and privacy** is taking on new dimensions in the context of hybrid warfare. AI systems need access to vast amounts of data to work effectively, including citizens' personal information. In peacetime, this would raise serious privacy concerns, but in the face of an existential threat, priorities can change.

The 100,000 attacks monthly context: With Ukraine facing approximately 100,000 cyberattacks monthly on government resources alone, the ethical calculus shifts. The Ministry of Digital Transformation's deployment of AI monitoring on all employee laptops represents this tension — necessary for security but raising privacy questions⁵².

- **The question of proportionality** arises when using AI for automated response to threats. How serious does the threat have to be to justify automatically cutting off the power supply to the area or blocking access to information resources?

Beyond algorithms, ethics extends to procurement. Trust in state institutions is a component of cybersecurity. Corruption scandals involving defense tech or critical infrastructure erode the trust necessary for public-private partnerships like Brave1 to function effectively.

6.2. Standardization of ethical behavior

The development of ethical standards for the use of AI in the Ukrainian security sector should take into account both universal principles and the specifics of the national context.

- **The principle of human autonomy** requires the preservation of the possibility of human intervention in any automated processes. This is especially important for decisions that may affect the lives and freedoms of citizens.

In practical implementation, this means the introduction of control systems according to two main models:

- *Human-in-the-loop* — when any critical decision requires direct human confirmation. This approach is mandatory for weapons systems and critical infrastructure.
- *Human-on-the-loop* — when the system acts autonomously, but the human operator retains continuous oversight and the ability to intervene at any time to adjust or cancel the system's actions. This approach is suitable for less critical applications while maintaining accountability.

Cyber Forces oversight structure: The new Cyber Forces will report directly to Commander-in-Chief Syrskyi and President Zelenskyy, establishing clear accountability chains for AI-enabled offensive cyber operations⁵³.

⁵² United24 Media (2025), supra note 22.

⁵³ Visit UKRAINE. (2025). Ukraine to create Armed Forces Cyber Forces: how they will protect the state in cyberspace. <https://visitukraine.today/es/blog/7035/ukraine-to-create-armed-forces-cyber-forces-how-they-will-protect-the-state-in-cyberspace#tasks-and-structure-of-the-cyber-forces>

- **The principle of transparency and explainability** requires AI systems to be able to provide clear explanations for their decisions. Explainable AI (XAI) technologies are becoming not just a technical requirement, but an ethical imperative.
- **The principle of fairness and impartiality** is especially important when using AI to identify threats or classify information. Algorithms should not discriminate against people on the basis of ethnicity, language, or religion.

6.3. Organizational and managerial challenges

Effective management of AI systems in the field of cybersecurity requires new organizational approaches and management practices.

Interagency coordination remains one of the most difficult challenges. The use of AI in cybersecurity requires coordinated interaction between:

- The Armed Forces of Ukraine and the new Cyber Forces Command, which are responsible for military cyber defense
- Security Service of Ukraine engaged in counterintelligence and anti-terrorist activities
- The Ministry of Internal Affairs through the Cyber Police
- Ministry of Digital Transformation, which coordinates civilian cyber infrastructure
- State Service for Special Communications and Information Protection
- Private IT companies providing technology solutions⁵⁴

The lack of a single coordination center leads to:

- Duplication of efforts and inefficient use of resources
- Inconsistencies in standards and approaches
- Weak exchange of information between subjects
- Slow response to new threats

Emerging challenges — prompt attacks and AI-guided malware: The emergence of AI-guided malware that queries AI systems in real-time for next steps, and prompt injection attacks against government AI systems, require new coordination mechanisms that traditional cybersecurity frameworks don't address⁵⁵.

Risk management of AI systems requires new assessment methodologies. Traditional approaches to risk management do not consider the specifics of algorithmic systems capable of self-learning and adaptation.

Ensuring the cybersecurity of the AI systems themselves is becoming a critical task. Paradoxically, systems designed to protect against cyber threats themselves become attractive targets for attacks.

⁵⁴ Danyk & Andreichuk (2025), *supra* note 10.

⁵⁵ CERT-UA. (2025). Emerging AI Threat Vectors Report. Composite reference from WRECKSTEEL analysis and H2 2024 analytics. <https://thehackernews.com/2025/04/cert-ua-reports-cyberattacks-targeting.html>

7. Strategic recommendations and future prospects

7.1. Conceptual Foundations of the National Strategy

Ukraine has a unique opportunity to become a leader in the responsible use of AI for cybersecurity. The experience of real combat use of these technologies provides advantages that no other democratic country has. With over 4,300 cyber incidents in 2024 and continued evolution of threats in 2025, Ukraine has developed unparalleled practical knowledge⁵⁶.

The integration of AI into the national cybersecurity strategy should be based on several key principles:

- *Adaptability* — systems must be able to quickly retrain and adapt to new types of threats, as demonstrated by CERT-UA's ability to track evolving Russian tactics
- *Resilience* — AI systems must remain operational even in case of partial damage or loss of some components
- *Interoperability* — different systems must interact with each other and with international partners, exemplified by Ukraine's integration into the EU Cybersecurity Reserve
- *Ethics* — all decisions must comply with democratic values and international law

7.2. Operational recommendations

The creation of the National AI Center for Cybersecurity will allow for the centralization of expertise, coordination of the efforts of different agencies, and ensuring uniform standards.

The functions of the center should include:

- Development of technical standards and ethical principles
- Certification of AI systems for use in critical infrastructure
- Training and retraining of personnel
- Coordination of research and development
- International cooperation⁵⁷
- Analysis of emerging threats like AI-generated malware and zero-click exploits
- Development of defenses against prompt injection attacks on government AI systems

The introduction of a system of regular audits of AI systems should become a mandatory requirement. Audits should assess:

- Technical reliability and safety

⁵⁶ CERT-UA. (2025). Annual Report 2024: 4,315 Cyber Incidents. <https://cip.gov.ua/en/news/cert-ua-minulogo-roku-opracuyvala-4315-kiberincidentiv>

⁵⁷ RAND Corporation (2024), *supra* note 1.

- Compliance with ethical principles
- Effectiveness in threat detection
- Impact on citizens' rights
- Resilience against adversarial attacks

The creation of a national platform for the exchange of threat data will maximize the effectiveness of AI systems through access to more complete and up-to-date information. Building on CERT-UA's experience analyzing 3,018 incidents in H1 2025, this platform should enable real-time sharing between government agencies, private sector, and international partners.

Addressing zero-click vulnerabilities systematically: With CERT-UA documenting sophisticated exploitation of CVE-2023-43770 and similar zero-click vulnerabilities, Ukraine needs a dedicated early warning system for such threats that leverages AI to identify exploitation patterns before they reach critical infrastructure⁵⁸.

Development of anti-AI-malware capabilities: As Russian hackers deploy AI-guided malware that adapts in real-time, Ukraine should prioritize development of AI systems specifically designed to detect and counter AI-generated attack code. The Wrecksteel malware case demonstrates this urgent need⁵⁹.

7.3. International cooperation and standardization

Ukraine should actively participate in the formation of international standards for the use of AI in cybersecurity, using its unique experience.

- **Cooperation with NATO** within the framework of artificial intelligence initiatives will allow integrating Ukrainian systems into alliance-wide cyber defense networks. The establishment of Cyber Forces aligned with NATO standards facilitates this integration⁶⁰.
- **Participation in EU programs** for the development of ethical AI will ensure access to funding and technology, as well as contribute to the harmonization of standards. Ukraine's official integration into the EU Cybersecurity Reserve on July 18, 2025, enabling rapid operational assistance from European rapid response teams during large-scale cyberattacks represents a major milestone⁶¹.
- **Partnership with democratic countries within the framework of the G7** and other formats will allow for the exchange of experience and coordination

⁵⁸ CERT-UA (2025), *supra* note 3.

⁵⁹ The Hacker News (2025), *supra* note 12

⁶⁰ NATO. (2023). AI Strategy Implementation Framework. https://www.nato.int/cps/en/natohq/official_texts_227237.htm

⁶¹ EU4Digital. (2025). Ukraine to receive EU cyber support in event of attacks <https://eufordigital.eu/ukraine-to-receive-eu-cyber-support-in-event-of-attacks/>

of approaches to regulation. Canada's contribution of 92 million UAH to strengthen Ukraine's cybersecurity exemplifies this cooperation⁶².

- **Sharing practical combat experience:** Ukraine's experience with AI-guided malware, zero-click exploits, and prompt injection attacks represents the most advanced real-world testing of cyber defense. This knowledge should be systematically shared with allies through NATO and bilateral channels.
- **The Brave1 model for international cooperation:** The Defense Tech Valley 2025 summit, which attracted over \$100 million in investment pledges from 40 countries, demonstrates how Ukraine can lead international cooperation in defense tech innovation while maintaining ethical oversight⁶³. Such cooperation is exemplary, provided that Ukraine upholds strict transparency and anti-corruption safeguards to ensure the trust of partners.

8. Conclusions and prospects of the study

8.1. Key achievements of Ukraine

The Ukrainian experience of using artificial intelligence in cybersecurity demonstrates several unique achievements of global importance⁶⁴.

- **The practical effectiveness** of AI systems in the context of a real hybrid war has confirmed theoretical assumptions about their usefulness. Systems for automatic detection of disinformation, protection against cyberattacks, and analysis of satellite images have shown high efficiency. CERT-UA's detection of AI-generated PowerShell scripts in the Wrecksteel malware campaign demonstrates practical AI-versus-AI combat capability⁶⁵.
- **The speed of adaptation** of Ukrainian developers and users to new technologies turned out to be significantly higher than predicted. This indicates the high potential of the Ukrainian IT industry and the readiness of society for technological changes. The Brave1 cluster's rapid growth to 3,300+ registered developments in just over a year exemplifies this agility⁶⁶.
- **Innovative approaches** to the integration of the public and private sectors have created a new model of cooperation, which can be useful for other countries. The Brave1 model of uniting manufacturers, military, government, investors and legal experts represents a replicable framework.

⁶² Mezha. (2025). Canada Provides \$3 Million CAD Cybersecurity Aid to Ukraine via Tallinn Mechanism <https://mezha.net/eng/bukvy/canada-provides-3-million-cad-cybersecurity-aid-to-ukraine-via-tallinn-mechanism/>

⁶³ Kyiv Post (2025), supra note 27.

⁶⁴ Danyk, Y., & Andreichuk, V. (2025). Artificial Intelligence in Countering Cyber Threats. [TACS 2025].

⁶⁵ The Hacker News (2025), supra note 12

⁶⁶ Brave1 Defense Tech Cluster. (2025). Official Statistics and Project Information. Ministry of Digital Transformation of Ukraine. <https://digitalstate.gov.ua/projects/tech/brave1>

- **Institutional innovation:** The creation of Cyber Forces as an independent command structure represents the most significant organizational achievement, positioning Ukraine at the forefront of military cyber capability development among democratic nations⁶⁷.

8.2. System Challenges and Risks

Along with the successes, the Ukrainian experience has revealed a number of systemic problems that need to be urgently solved:

- **The lack of comprehensive regulation** creates risks of uncontrolled technology development and potential abuse. While Law №4336 established unified incident response coordination, gaps remain in AI-specific regulation⁶⁸.
- **The ethical dilemmas** of using AI to monitor citizens (such as the Ministry of Digital Transformation's laptop monitoring system) and automated decision-making that affect people's lives remain unresolved⁶⁹.
- **Technological dependence** on foreign platforms and solutions creates strategic risks to national security. Ukrainian cybersecurity customers' preference for international vendors over domestic firms highlights this vulnerability⁷⁰.
- **Personnel challenges:** Despite market growth to \$138 million in 2024 with projections of \$208.80 million by 2029, talent retention against private sector competition remains problematic⁷¹.
- **Emerging AI threats:** The appearance of AI-guided malware, prompt injection attacks, and AI-generated phishing at industrial scale represents threats that traditional cybersecurity frameworks were not designed to address⁷².

8.3. Development prospects

Short-term prospects (1-2 years):

- Adoption of basic legislation on artificial intelligence with specific provisions for AI-generated threats
- Full operationalization of the Cyber Forces Command structure

⁶⁷ CSIS. (2025). Unpacking Ukraine's Future Cyber and Space Forces. <https://www.csis.org/analysis/unpacking-ukraines-future-cyber-and-space-forces#>

⁶⁸ Verkhovna Rada of Ukraine. (2025). Law No. 4336 <https://zakon.rada.gov.ua/laws/show/4336-20#Text>

⁶⁹ ECNL. (2025). Safeguarding human rights in the sphere of AI in Ukraine. <https://ecnل.org/impact-story/safeguarding-human-rights-sphere-ai-ukraine#>

⁷⁰ The Record. (2025). Ukrainian cyber market grows amid war but still lacks support and funding, report says. <https://therecord.media/ukraine-cybersecurity-market-study-datadriven>

⁷¹ Statista. (2025). Cybersecurity — Ukraine. <https://www.statista.com/outlook/tmo/cybersecurity/ukraine>

⁷² CERT-UA (2025), *supra* note 3.

- Development of national ethical standards incorporating lessons from Brave1's legal oversight model
- Establishment of systematic defenses against zero-click vulnerabilities and AI-guided malware
- Integration of Ukrainian cyber capabilities into NATO frameworks

Medium-term prospects (3-5 years):

- Integration of Ukrainian AI systems into Euro-Atlantic security networks
- Creating a national AI development and production ecosystem building on Brave1's success
- Training a new generation of specialists combining AI, cybersecurity, and military expertise
- Development of indigenous AI platforms reducing dependence on foreign technologies
- Export of Ukrainian defensive AI solutions and practical experience to allied nations

Long-term perspectives (5-10 years):

- Ukraine's emergence as a regional leader in the field of ethical AI for defense applications
- Export of Ukrainian solutions and experience to other countries
- Formation of new international standards based on Ukrainian combat-tested experience
- Establishment of Ukraine as the global center for AI-enabled cyber defense innovation
- Full technological sovereignty in critical AI and cybersecurity capabilities

8.4. Conceptual conclusions

The study confirms several fundamental theses about the role of AI in modern cybersecurity:

- **Artificial intelligence is not a neutral tool.** Its deployment is inherently value-laden, reflecting the priorities, ethical frameworks, and strategic objectives of those who design and deploy it. This fundamental insight underscores why AI governance in democratic societies must prioritize transparency and accountability. The Brave1 model demonstrates how ethical oversight can be integrated into defense tech development.
- **Hybrid threats require hybrid responses.** Traditional approaches to cybersecurity based on static protection systems are proving insufficient against adaptive algorithmic attacks. Ukraine's experience facing 100,000+ monthly attacks on government systems alone validates this conclusion⁷³.

⁷³ United24 Media (2025), *supra* note 22.

- **International cooperation is critical.** No country can effectively counter modern cyber threats alone. AI enhances both defense capabilities and attack potential. Ukraine's integration into the EU Cybersecurity Reserve and cooperation with NATO demonstrate the practical value of alliance cooperation⁷⁴.
- **Ukrainian experience has global value.** The practical application of AI in a real hybrid war provides unique knowledge that can be useful for the entire global community. Ukraine is the first democratic nation to face AI-guided malware, prompt injection attacks at government scale, and coordinated AI-enabled hybrid operations — making its experience invaluable for allies⁷⁵.
- **The AI revolution in cyber warfare is accelerating.** From AI-generated malware to zero-click exploits to prompt injection attacks, the threat landscape is evolving faster than traditional defense procurement cycles. Only adaptive, AI-enabled defense can keep pace.

8.5. Directions for further research

The presented study opens up several promising areas for further study:

- **Technical aspects:** The study of methods to protect AI systems from competitive attacks and data poisoning requires in-depth analysis. Specific research on defending against prompt injection attacks and AI-guided malware adaptation is urgently needed.
- **Legal issues:** The development of detailed mechanisms of responsibility for the actions of autonomous systems requires an interdisciplinary approach. The Cyber Forces' accountability structure provides a starting point for this research.
- **Ethical dilemmas:** Balancing security and privacy in the face of existential threats requires new theoretical approaches. The case of monitoring 100,000 monthly attacks while deploying surveillance on government employee laptops presents a real-world ethical laboratory.
- **International Relations:** The impact of AI on strategic stability and international security is a relevant topic for further research. Ukraine's experience should inform NATO and EU policy development.
- **Emerging threat vectors:** Systematic study of AI-guided malware evolution, zero-click vulnerability exploitation patterns, and prompt injection attack methodologies based on Ukraine's frontline experience.

⁷⁴ Digital State UA. (2025). Ukraine Gains Access to the EU Cybersecurity Reserve <https://digitalstate.gov.ua/news/govtech/ukraine-gains-access-to-the-eu-cybersecurity-reserve-operational-support-in-the-event-of-large-scale-attacks>.

⁷⁵ Cyble (2025), supra note 35

- **Public-private partnership models:** Analysis of the Brave1 ecosystem's effectiveness in accelerating defense innovation while maintaining ethical standards could inform policy in other democracies.
- **Talent development:** Investigation of effective models for training cybersecurity professionals who combine AI expertise with operational military knowledge, drawing on Ukraine's accelerated wartime experience.

References

- Allen, G. C., & Husain, R. (2023). *Artificial intelligence and national security*. Center for a New American Security. <https://www.belfercenter.org/publication/artificial-intelligence-and-national-security>
- Brave1 Defense Tech Cluster. (2025). *Official statistics and project information*. Ministry of Digital Transformation of Ukraine. <https://digitalstate.gov.ua/projects/tech/brave1>
- Brave1. (2025). *Ukraine officially launches Brave1 Market — First online defense technology marketplace*. Ministry of Digital Transformation. <https://digitalstate.gov.ua/news/tech/brave1-market-ukrayina-zapuskaye-marketpleys-viyskovykh-innovatsiy>
- Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitsoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Amodei, C., Meserole, C., Yang, E., Brown, T., & Amodei, D. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. arXiv. <https://arxiv.org/abs/1802.07228>
- CERT-UA. (2025). *CERT-UA recorded 4315 cyber incidents in 2024*. State Service of Special Communications and Information Protection of Ukraine. <https://cip.gov.ua/en/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv>
- CERT-UA. (2025). *Russian cyber operations analytics for H2 2024 [TLP:CLEAR]*. State Service of Special Communications and Information Protection of Ukraine. <https://cip.gov.ua/services/cm/api/attachment/download?id=68768>
- Cisco. (2024). *Cybersecurity readiness index 2024*. <https://www.cisco.com/c/en/us/products/security/cybersecurity-readiness-index.html>
- Cyble. (2025). *Government Sector Bears the Brunt of Cyberattacks in Ukraine: Report*. <https://cyble.com/blog/ukraine-cyberthreat-landscape-2024/>
- Danyk, Yu., Andreichuk, V. (2024). *Shtuchnyi intelekt u sferi natsionalnoi bezpeky ta oborony: mozhlyvosti ta vyklyky, protydiia ryzykam i zahroza* [Artificial intelligence in national security and defense: Opportunities and challenges, risk and threat mitigation]. *Naukovyi zbirnyk Ukrainskoho Vilnoho Universytetu* [Scientific collection of the Ukrainian Free University], 2023/24, Vol. 24, pp. 191–209. [in Ukrainian]
- Danyk, Yu., Andreichuk, V. (2025). *Shtuchnyi intelekt u protydii kiberzahrozam v hibrnykh vysokotekhnolohichnykh konfliktakh* [Artificial intelligence in countering cyber threats in hybrid high-tech conflicts]. *Materialy mizhnarodnoi konferentsii TACS 2025* [Materials of the international conference TACS 2025], Kyiv, 29 Mai 2025, pp. 68–79. [in Ukrainian]
- Dark Reading. (2025). *Putin's attacks on Ukraine rise 70%, with little effect*. <https://www.dark-reading.com/threat-intelligence/putin-cyberattacks-ukraine-rise-little-effect>
- Detector Media. (2024). *Media monitoring Ukraine*. <https://detector.media/>

- DSEI. (2025). *Feature: Ukraine's Brave1 highlights progress, invites collaboration*. <https://www.dsei.co.uk/news/feature-ukraines-brave1-highlights-progress-invites-collaboration>
- ENISA. (2025). *Threat landscape report 2025*. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>
- ECNL. (2025). *Safeguarding human rights in the sphere of AI in Ukraine*. European Center for Not-for-Profit Law. <https://ecnl.org/impact-story/safeguarding-human-rights-sphere-ai-ukraine>
- European Parliament and Council of the European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union, L 1689. <https://artificialintelligenceact.eu/the-act/>
- Ferrara M. (2025). *Data Poisoning and Artificial Intelligence Modeling: Theoretical Foundations and Defensive Strategies*. https://ceur-ws.org/Vol-4031/04_regular.pdf
- Future of Life Institute. (2024). *AI policy — National and international governance*. <https://futureoflife.org/ai-policy/>
- The Hacker News. (2024). *CERT-UA warns of phishing attacks targeting Ukraine's defense and security forces*. <https://thehackernews.com/2024/12/cert-ua-warns-of-phishing-attacks.html>
- The Hacker News. (2025). *CERT-UA reports cyberattacks targeting Ukrainian state systems with WRECKSTEEL malware*. <https://thehackernews.com/2025/04/cert-ua-reports-cyberattacks-targeting.html>
- The Hacker News. (2025). *CERT-UA warns of cyber scams using fake AnyDesk requests for fraudulent security audits*. <https://thehackernews.com/2025/01/cert-ua-warns-of-cyber-scams-using-fake.html>
- Hoffman W., Kim H.M. (2023) *Reducing the Risks of Artificial Intelligence for Military Decision Advantage*. <https://cset.georgetown.edu/publication/reducing-the-risks-of-artificial-intelligence-for-military-decision-advantage/>
- Institute for Media Development (IMI). (2025). *Cyber attacks on Ukraine spiked by 70% in 2024*. <https://imi.org.ua/en/news/cyber-attacks-on-ukraine-spiked-by-70-in-2024-i65939>
- International Policy Digest. (2025). *Ukraine's Brave1 is racing to redefine warfare* [Interview with Artem Moroz, Deputy Head of Partnerships]. <https://intpolicydigest.org/ukraines-brave1-is-racing-to-redefine-warfare/>
- Kyiv Post. (2025). *Ukraine secures over \$100M in defense tech investment at Brave1 Defense Tech Valley 2025*. <https://www.kyivpost.com/post/60491>
- Mezha. (2025). *Canada Provides \$3 Million CAD Cybersecurity Aid to Ukraine via Tallinn Mechanism* <https://mezha.net/eng/bukvy/canada-provides-3-million-cad-cybersecurity-aid-to-ukraine-via-tallinn-mechanism/>
- National Institute of Standards and Technology. (2024). *Artificial intelligence risk management framework: Generative artificial intelligence profile (NIST AI 600-1)*. U.S. Department of Commerce. <https://doi.org/10.6028/NIST.AI.600-1>
- NATO. (2023). *Summary of NATO's artificial intelligence strategy*. https://www.nato.int/cps/en/natohq/official_texts_227237.htm
- OECD. (2019). *OECD AI principles*. <https://oecd.ai/en/ai-principles>

- President of Ukraine. (2021). Decree No. 447/2021. *On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine"*. <https://www.president.gov.ua/documents/4472021-40013> [in Ukrainian]
- Probasco, E., Toner, H., Burtell, M., & Rudner, T. G. J. (2025). *AI for military decision-making: Harnessing the advantages and avoiding the risks*. Center for Security and Emerging Technology. <https://cset.georgetown.edu/publication/ai-for-military-decision-making/>
- RAND Corporation. (2024). *AI and national security: Research topics and risks*. <https://www.rand.org/topics/artificial-intelligence.html>
- The Report. (2025). Ukrainian cyber market grows amid war but still lacks support and funding, report says. <https://therecord.media/ukraine-cybersecurity-market-study-datadriven>
- Statista. (2025). *Cybersecurity — Ukraine*. <https://www.statista.com/outlook/tmo/cybersecurity/ukraine>
- StopFake. (2024). *Fact-checking Ukraine*. <https://www.stopfake.org/>
- The Cyber Express. (2025). *Ukraine Reports 48% Jump in Cyber Incidents in H2 2024, but 77% Drop in High-Severity Incidents*. <https://thecyberexpress.com/cyber-incidents-in-h2-2024-ukraine/>
- Ukrinform. (2025). *Canada allocates €92 million to Ukraine to strengthen cybersecurity* <https://www.ukrinform.net/rubric-society/4039965-canada-allocates-92-million-to-ukraine-to-strengthen-cybersecurity.html>
- United24 Media. (2025). *Inside Brave1, the tech hub powering Ukraine's battlefield innovations*. <https://united24media.com/war-in-ukraine/inside-brave1-the-tech-hub-powering-ukraines-battlefield-innovations-7011>
- United24 Media. (2025). *Ukraine's Brave1 program attracts 45 foreign firms to trial drones, AI, and laser weapons*. <https://united24media.com/latest-news/ukraines-brave1-program-attracts-45-foreign-firms-to-trial-drones-ai-and-laser-weapons-10655>
- Verkhovna Rada of Ukraine. (2025). *Ukraine Parliament Approves Cyber Forces Legislation (Bill No. 12349, October 9, 2025)*. <https://www.rada.gov.ua/news/razom/266780.html>
- Visit UKRAINE. (2025). *Ukraine to create Armed Forces Cyber Forces: how they will protect the state in cyberspace*. <https://visitukraine.today/es/blog/7035/ukraine-to-create-armed-forces-cyber-forces-how-they-will-protect-the-state-in-cyberspace#tasks-and-structure-of-the-cyber-forces>