DOI: https://doi.org/10.30525/2256-0742/2026-12-4-352-359

ECONOMIC CYBER-ESPIONAGE IN THE CONTEXT OF GLOBAL DIGITAL TRANSFORMATION AND THE WAR IN UKRAINE: RISKS TO ECONOMIC SECURITY, CYBER THREATS AND REGULATORY CHALLENGES

Oleksandr Makhlai[1], Dmytro Bulatin[2], Yurii Vykhodets[3]

Abstract. This article examines economic cyber-espionage as a systemic threat to economic security, considering it in the context of global digital transformation and the growing reliance of modern economies on information technology. It explores how cyber-espionage has evolved from an intelligence-related activity to become an instrument of economic competition, technological rivalry and geopolitical influence. Particular attention is paid to the mechanisms involved in obtaining confidential commercial information, intellectual property, technological developments and strategic economic data by exploiting vulnerabilities in digital infrastructures.

The research identifies the key features of economic cyber-espionage, such as its transnational nature, the anonymity of the perpetrators, the long-term persistence of cyber operations and the involvement of state-sponsored advanced persistent threat (APT) groups. The article analyses the economic consequences of cyber-espionage, including losses associated with intellectual property theft, disruption to innovation processes, reduced competitive advantage and increased cybersecurity costs.

The article pays special attention to the role of cyber-espionage in the context of Russia's war against Ukraine, where cyber operations have become an integral part of hybrid warfare. The article shows that cyber-attacks on Ukrainian government institutions, critical infrastructure, defence enterprises and economic entities pose security threats and are attempts to undermine economic resilience and acquire valuable strategic information.

The study emphasises the challenges of international legal regulation and institutional responses to economic cyber-espionage. The lack of universally recognised rules governing state-sponsored cyber operations, the difficulty of attributing cyber attacks, and the limitations of international co-operation mechanisms all significantly reduce the effectiveness of countermeasures.

The article concludes that economic cyber-espionage has become a significant factor in global economic security. In order to protect digital economies and ensure sustainable development, it is essential to strengthen international co-operation, develop unified regulatory approaches, improve cybersecurity governance and integrate cyber resilience into national economic strategies.

Keywords: economic cyber-espionage, economic security, digital transformation, cybersecurity, intellectual property protection, cyber threats, advanced persistent threats, hybrid warfare, Ukraine.

JEL Classification: O33, F52, K42

Received on: June 25, 2026 **Accepted on:** August 23, 2026 **Published on:** September 28, 2026

[1] Bohdan Khmelnytskyi National Academy of the State Border Service of Ukraine, Ukraine *(corresponding author)*
E-mail: al_m@ukr.net
ORCID: https://orcid.org/0000-0002-8201-3387
[2] The National Academy of the National Guard of Ukraine, Ukraine
E-mail: bulatin.dima@gmail.com
ORCID: https://orcid.org/0000-0002-0200-2822
[3] National Academy of Internal Affairs, Ukraine
E-mail: navs2026@ukr.net
ORCID: https://orcid.org/0009-0008-1312-9248

1. Introduction

The rapid development of digital technologies has fundamentally altered the structure of global economic relations. Digital platforms, cloud computing, artificial intelligence and interconnected information systems have become integral to modern economic activity, fostering innovation, international collaboration and increased productivity. However, increasing dependence on digital infrastructures has also generated new categories of economic risk, such as unauthorised access to strategic information resources.

One of the most dangerous manifestations of these risks is economic cyber-espionage, which combines the technological capabilities of cyberspace with the traditional objectives of intelligence activities, namely the acquisition of valuable economic information. Unlike conventional cybercrime, which is usually motivated by direct financial gain, economic cyber-espionage primarily focuses on acquiring strategic advantages by stealing intellectual property, industrial secrets, scientific developments and confidential business information (Fidler, 2013).

This phenomenon has become much more significant due to growing competition between states in high-technology sectors. Access to advanced technologies, research results, defence-related innovations and industrial developments has become a key factor in determining a country's economic competitiveness. Consequently, cyber operations targeting economic entities are being used more and more as instruments of geopolitical rivalry and technological competition.

According to the World Economic Forum, cybersecurity risks continue to be among the most significant global challenges, affecting economic stability, investment activity and trust in digital markets (World Economic Forum, 2025). Global economic losses caused by cyber incidents are continuing to grow, demonstrating that cybersecurity is now an essential element of economic governance, as well as a technical issue.

In the context of Russia's full-scale war against Ukraine, the relevance of studying economic cyber-espionage has increased significantly. The Ukrainian experience shows that cyberspace has become a separate domain of conflict, with cyber operations accompanying traditional military actions. Cyber-attacks against government institutions, energy facilities, financial organisations, defence enterprises and technology companies not only aim to disrupt operations, but also to obtain strategic information and weaken economic resilience (Shkuta, 2025).

The scientific problem addressed in this article is determined by the contradiction between the increasing economic importance of digital information resources and the insufficient development of international mechanisms for preventing and responding to economic cyber-espionage. Despite the existence of various cybersecurity strategies and regulatory initiatives, there remains no universally accepted legal framework capable of effectively addressing state-sponsored cyber operations targeting economic interests (Shkuta, 2022).

This research aims to analyse economic cyber-espionage as a contemporary threat to economic security in the context of global digital transformation and wartime challenges. It seeks to identify the phenomenon's technological and organisational characteristics and examine regulatory and institutional mechanisms for counteracting it.

To achieve this objective, the following research tasks are defined:

– To clarify the conceptual characteristics of economic cyber-espionage and distinguish it from other forms of cybercrime.
– To analyse the economic consequences of cyber-espionage for states, enterprises, and innovation systems.
– To examine modern technological instruments used in economic cyber operations.
– To assess the role of cyber-espionage in the context of Russia's war against Ukraine.
– To identify international regulatory challenges and propose directions for improving cybersecurity governance.

2. Methodology

The methodological framework of the research combines interdisciplinary approaches that integrate legal, economic, and cybersecurity perspectives.

The present study employs a system analysis method to examine economic cyber-espionage as a complex phenomenon involving technological, economic, political and legal components. This approach facilitates the identification of relationships between cyber threats and economic security mechanisms.

The comparative legal method is utilised to analyse international approaches to regulating cyber operations, including cybersecurity strategies developed by the European Union, the United States, and international organisations.

The present study employs a criminological and security analysis approach to determine the characteristics of cyber-espionage actors, including state-sponsored groups, advanced persistent threat (APT) organisations, and technologically sophisticated criminal networks.

The research employs a case study analysis of significant cyber incidents affecting economic systems, including cyber operations against Ukrainian institutions during the Russian invasion, attacks targeting intellectual property, and large-scale corporate data breaches (Shkuta, 2024).

The empirical basis of the research consists of analytical reports of international organisations, cybersecurity companies, governmental institutions, and academic publications indexed in international databases.

The methodological approach adopted herein facilitates the consideration of economic cyber-espionage not only as a cybersecurity problem in its own right, but also as a factor influencing international economic competition, investment security, innovation development, and national resilience.

3. Results and Discussion

3.1. Economic Cyber-Espionage as a Threat to Digital Economic Security

The global economy's transformation into a digitally dependent system has fundamentally altered the nature of economic competition. Data, technological knowledge, intellectual property and innovative solutions have become strategic economic assets, comparable to traditional material resources. Consequently, the unauthorised acquisition of such information via cyberspace has become an effective means of gaining competitive advantage at both the corporate and state levels.

Economic cyber-espionage differs from conventional cybercrime primarily due to its strategic orientation. While financially motivated cyberattacks generally seek immediate economic benefits through fraud, extortion or unauthorised financial transactions, cyber-espionage operations aim to obtain long-term advantages by covertly accessing valuable information resources. Main targets include technological developments, industrial designs, scientific research results, trade secrets, business strategies and confidential government economic data (Fidler, 2013).

The economic consequences of cyber-espionage extend far beyond direct financial losses. The theft of intellectual property can reduce incentives for innovation, undermine the attractiveness of investment and weaken the competitive position of companies operating in technology-intensive markets. For states, the systematic loss of technological knowledge can result in dependence on foreign innovations and a deterioration in strategic economic autonomy.

According to the IBM Security report, the average global cost of a data breach was 4.88 million USD in 2024, highlighting the growing economic importance of cybersecurity risks (IBM Security, 2024). However, the actual economic impact of cyber-espionage is considerably higher, as many organisations avoid publicly reporting incidents due to concerns about their reputation, potential market losses and investor confidence.

The high level of latency is one of the defining characteristics of economic cyber-espionage. Unlike traditional economic crimes, the consequences of which are often immediately visible, cyber-espionage operations may remain undetected for months or even years. Advanced Persistent Threat (APT) groups are specifically designed to maintain long-term access to compromised systems while minimising the risk of detection (Shkuta, 2025).

Consequently, the issue of economic cyber-espionage should be regarded not solely as a cybersecurity challenge, but also as a structural threat to economic stability, technological development, and international competitiveness.

3.2. Technological Mechanisms and Actors of Economic Cyber-Espionage

Modern economic cyber-espionage operations demonstrate a significant increase in technological complexity. Such operations are typically carried out by state-sponsored groups, private hacker organisations, intelligence agencies and proxy actors, all of whom operate within a coordinated strategic framework.

A defining feature of contemporary cyber-espionage is the activity of Advanced Persistent Threat (APT) groups. These groups combine technical expertise, financial resources and strategic objectives, enabling them to carry out long-term operations against specific targets.

According to an analysis by Google Threat Intelligence, various state-linked APT groups demonstrate different strategic models of cyber activity. Chinese-linked groups traditionally focus on technological acquisition and intellectual property theft, targeting sectors such as aerospace, telecommunications, engineering and advanced manufacturing. In contrast, Russian-linked groups combine intelligence gathering with destructive capabilities directed against critical infrastructure and strategic institutions. Meanwhile, North Korean and Iranian groups are increasingly using cyber operations to obtain financial resources and support state programmes (Google Cloud Security, 2025).

The most common technological instruments of economic cyber-espionage include:

– Spear-phishing attacks, which involve personalised social engineering techniques aimed at obtaining authentication data or introducing malicious software;
– zero-day vulnerability exploitation, allowing attackers to compromise systems before security updates become available;
– supply chain attacks, where attackers compromise less protected suppliers to gain access to larger organisations;
– insider threats, involving employees or contractors who intentionally or unintentionally facilitate unauthorised access;
– malware-based operations, including spyware, remote access tools, and data-exfiltration mechanisms.

Particular attention should be paid to the growing role of artificial intelligence (AI) technologies. AI significantly enhances the capabilities of cyber actors, enabling the automated detection of vulnerabilities, the generation of convincing phishing content, the creation of deepfake materials and the improvement of social engineering methods. Consequently, AI contributes to the increased scale, speed and adaptability of cyber-espionage operations.

The combination of technological innovation and strategic objectives makes economic cyber-espionage one of the most complex threats to the contemporary digital economy.

3.3. Economic Cyber-Espionage in the Context of Russia's War Against Ukraine

The large-scale Russian invasion of Ukraine has demonstrated that cyberspace has become a distinct dimension of modern warfare. Cyber operations against Ukraine have been conducted in parallel with conventional military action, targeting government institutions, energy systems, financial organisations, defence enterprises and communication networks.

The economic dimension of these attacks is of particular significance, given that cyber operations are aimed not only at disrupting infrastructure but also at weakening economic resilience, obtaining strategic information, and reducing technological capabilities.

Russian cyber groups, including state-affiliated APT organisations, have conducted numerous operations involving espionage, the deployment of destructive malware, and the collection of intelligence. These activities demonstrate the integration of cyber capabilities into wider military and geopolitical strategies.

The Ukrainian experience demonstrates several important characteristics of wartime economic cyber-espionage:

Firstly, cyber operations are increasingly being directed against critical economic infrastructure. Energy systems, transportation networks, financial institutions and industrial enterprises have become strategic targets because disrupting them would have significant economic consequences.

Secondly, cyber-espionage is employed to gather information about defence production, technological capabilities, international co-operation and economic planning.

Thirdly, cyber operations can contribute to psychological and economic pressure by undermining confidence in digital systems and raising the cost of maintaining cybersecurity.

According to Ukraine's cybersecurity authorities, the number of cyber incidents has increased substantially since the start of Russia's full-scale invasion, confirming that cyberspace has become an integral part of hybrid warfare.

Therefore, economic cyber-espionage during wartime should be understood as a means of strategically weakening an opponent's economic potential, rather than merely as a violation of information security.

3.4. Intellectual Property Protection and Innovation Risks

One of the most significant economic consequences of cyber-espionage is the unauthorised acquisition of intellectual property. In knowledge-based economies, technological innovation is a key driver of competitive advantage and economic growth.

The theft of intellectual property via cyber means enables perpetrators to cut research and development costs, speed up technological advancement and undermine competitors. This can result in countries and companies that invest significant resources in innovation losing out on economic benefits due to unauthorised technological transfers.

The problem is especially relevant for sectors such as:

- Artificial intelligence;
- biotechnology;
- aerospace technologies;
- semiconductor production;
- defence industries;
- renewable energy technologies.

Economic cyber-espionage therefore has a direct impact on innovation ecosystems. It reduces the incentive to invest in research, increases cybersecurity expenditure and creates uncertainty regarding international technological co-operation.

Protecting intellectual property in the digital environment requires technical cybersecurity measures, as well as effective institutional mechanisms that combine economic regulation, international co-operation and legal protection.

3.5. International Regulatory Challenges and Attribution Problems

Despite the growing scale of economic cyber-espionage, international regulation remains insufficiently developed. One of the main issues is the lack of universally accepted legal standards that define the responsibility of states for cyber operations aimed at acquiring economic information.

Economic cyber-espionage largely remains within the so-called 'grey zone' of international law. Unlike traditional armed aggression, cyber operations rarely involve physical destruction, which makes their legal classification significantly more complicated.

A central challenge is cyber attribution, which is the process of reliably identifying the perpetrators of cyber attacks and determining their affiliations. Modern

cyber actors often use proxy structures, compromised infrastructure, false digital identities and technical methods designed to hide their origins.

Difficulties in establishing attribution reduce the effectiveness of international response mechanisms because diplomatic, economic and legal measures require sufficient certainty regarding responsibility.

Furthermore, international co-operation is complicated when cyber operations are conducted by state-affiliated actors. This is because traditional mechanisms of extradition and mutual legal assistance are often ineffective, as the state in which the perpetrators are operating may refuse to co-operate or provide political protection.

Therefore, improving global cybersecurity governance requires new approaches that can address the specific characteristics of digital economic threats.

3.6. Economic Indicators of Cybercrime, Cyber-Espionage and Cybersecurity Investment

A more complete assessment of economic cyber-espionage requires an analysis of quantitative indicators reflecting both the scale of cyber-related economic losses and the resources allocated to preventing them. At the same time, methodological caution is necessary. Global estimates of the damage caused by cybercrime include a broad range of consequences, such as the theft of funds and data, intellectual property, and business interruption, as well as lost productivity, forensic and recovery costs, and reputational harm. Therefore, they cannot be interpreted as a direct monetary estimate of cyber-espionage alone. However, given that theft of intellectual property and state-sponsored hostile cyber activity form part of the underlying loss model, these indicators provide a useful macroeconomic proxy for assessing the growing economic burden of the cyber threat environment (Cybersecurity Ventures, 2025).

The data show that the macroeconomic burden of cybercrime is increasing exceptionally rapidly. The estimated annual cost has almost doubled between 2020 and 2025. This is an economically relevant trend for cyber-espionage, as contemporary loss assessments explicitly include intellectual property theft, compromised commercial and financial information, business process disruption, and recovery expenditure. In this sense, cyber-espionage results in an immediate loss of confidentiality, as well as a delayed competitive effect. The victim may lose exclusivity over research results, technological know-how, market strategies or industrial information, while the beneficiary can reduce their own research and development costs and accelerate their entry to the market.

The simultaneous growth in cyber losses and defensive expenditure highlights a structural imbalance in the digital economy. Increased investment in cybersecurity does not automatically lead to a reduction in aggregate losses, as the attack surface grows alongside cloud migration, platformisation, artificial intelligence, supply-chain interdependence, and the commercialisation of offensive cyber tools. Consequently, cybersecurity expenditure should be viewed as an investment in economic resilience,

Table 1
Estimated Global Economic Losses from Cybercrime and Cyber-Enabled Economic Threats, 2020–2025

Year	Estimated global losses, trillion USD	Status / methodological note
2020	5.2	Model-based estimate*
2021	6.0	Published estimate
2022	6.9	Model-based estimate*
2023	8.0	Model-based estimate*
2024	9.5	Published estimate
2025	10.5	Published estimate

*The 2020, 2022 and 2023 values are analytical interpolations derived from the published Cybersecurity Ventures trajectory of approximately 15% annual growth between 6 trillion USD in 2021 and 10.5 trillion USD in 2025. They should therefore be treated as trend estimates rather than independently observed annual statistics.

Source: compiled by the authors on the basis of Cybersecurity Ventures (2020; 2024; 2025).

Table 2
Global Investment in Information Security and Cybersecurity, 2021–2025

Period	Spending, billion USD	Indicator
2021–2025	>1,750 (cumulative)	Cybersecurity products and services; forecast cumulative spending
2023	162.1	Information-security end-user spending
2024	183.9	Information-security end-user spending
2025	211.6–213.0	Information-security end-user spending; forecast/revised forecast

Source: Cybersecurity Ventures; Gartner. Gartner's 2024 forecast placed worldwide information-security end-user spending at 183.9 billion USD in 2024 and 211.6 billion USD in 2025, while its June 2025 update estimated 2025 spending at approximately 213 billion USD. Cybersecurity Ventures estimated cumulative cybersecurity spending above USD 1.75 trillion for 2021–2025.

rather than merely an operating cost of information technology. The benefits of such an investment include avoiding business interruption, protecting intellectual property, preserving investor and consumer confidence, and reducing systemic risks for critical sectors.

3.7. Comparative Analysis of Cybersecurity Resilience and Digital Investment in Selected European Countries

A European comparison shows that national responses to cyber risks vary significantly in terms of scale, institutional design and investment capacity. To ensure comparability, Table 3 uses the European Commission's Digital Decade country reports. The financial indicators refer to broader national digital transformation roadmaps and funds, rather than cybersecurity expenditure alone. Accordingly, they are used as indicators of the resource base within which cyber resilience is developed. This distinction is important because cybersecurity is becoming an integral part of wider programmes focusing on digital infrastructure, artificial intelligence, cloud services, the digitalisation of the public sector, and the sovereignty of critical technologies.

The comparison reveals three analytically significant patterns. Firstly, the largest European economies, particularly Germany and France, have substantially greater absolute investment capacity. This enables them to develop critical technologies, digital infrastructure and cyber resilience simultaneously. Secondly, smaller, highly digitalised states demonstrate that institutional maturity can compensate for a smaller absolute resource base to some extent. Estonia and the Netherlands, for example, rely heavily on advanced digital public services, innovation ecosystems and integrated governance. Thirdly, Poland and Croatia's experience shows that rapid infrastructure development must be accompanied by investment in cybersecurity skills, SME resilience, and organisational capacity. Therefore, the effectiveness of a country's cyber resilience cannot be assessed solely by the amount it spends; institutional quality, human capital, regulatory implementation and the ability to integrate cybersecurity into economic policy are equally important factors.

This European experience is particularly relevant for Ukraine. In the face of prolonged military aggression, investment in cybersecurity serves dual economic and security functions. It safeguards critical infrastructure and public administration, while also preserving technological assets, ensuring business continuity and investment confidence, and protecting the integrity of defence-related innovation. Therefore, the most appropriate model is not the isolated financing of technical protection, but rather the integration of cyber resilience into national economic recovery, industrial policy, innovation policy, and intellectual property protection.

4. Conclusions

In the era of global digital transformation, economic cyber-espionage has become one of the most significant challenges to economic security. The growing reliance of economic processes on digital infrastructure, cloud technologies, artificial intelligence and interconnected information systems has not only created new opportunities for economic development, but also for gaining unauthorised competitive advantages through cyberspace.

Unlike traditional cybercrime, economic cyber-espionage is characterised by a strategic approach, long-term goals and the involvement of highly organised actors, including state-sponsored Advanced Persistent Threat (APT) groups. Its main aim is not to make an immediate financial gain, but to acquire strategically valuable information, such as intellectual property, technological developments, industrial secrets and confidential economic data.

The analysis shows that the economic impact of cyber-espionage goes beyond direct financial losses. Such activities can undermine innovation potential, reduce the competitiveness of enterprises, increase cybersecurity expenditure, weaken investment

Table 3
Selected European Countries: Digital Investment and Cybersecurity Position, 2025

Country	Digital-policy investment indicator	Cybersecurity / resilience assessment
Germany	102.1 bn roadmap; 46.8 bn public	Large-scale advanced-technology base; need to further strengthen cyber resilience
France	18.6 bn roadmap; 11.1 bn public	Strong digital infrastructure and AI capacity; business digitalisation remains uneven
Poland	12.4 bn roadmap (1.47% GDP)	Cybersecurity measures deployed across government; digital skills and advanced business adoption remain challenges
Netherlands	5.25 bn roadmap; 5.22 bn public	Strong innovation base; cybersecurity included among strategic technology priorities
Croatia	634.73 m roadmap (0.74% GDP)	Strong progress in digital infrastructure and cybersecurity; SME digitalisation remains a constraint
Estonia	Budget not fully specified	Highly digital public sector; strong digital ecosystem but persistent ICT/cybersecurity skills constraints

Source: compiled by the authors from European Commission, Digital Decade 2025 Country Reports. The figures represent national digital-transformation roadmaps and should not be interpreted as stand-alone cybersecurity budgets.

attractiveness and create risks for national economic sovereignty. In knowledge-based economies, the unauthorised acquisition of technological information can have a significant impact on global markets and alter the balance of economic competition. The quantitative indicators examined in this study show that global cybercrime-related losses approached 10.5 trillion USD annually by 2025, while worldwide information security spending exceeded 200 billion USD per year. This confirms that cyber risk has become a macroeconomic factor rather than a purely technical problem.

The development of artificial intelligence, automation technologies and advanced social engineering methods increases the effectiveness and scalability of cyber-espionage operations. When combined with geopolitical objectives, these technological capabilities transform cyber-espionage into a significant instrument of economic influence and strategic competition between states.

Ukraine's experience of full-scale Russian aggression confirms that economic cyber-espionage has become an integral element of hybrid warfare. Attacks on government institutions, critical infrastructure, defence enterprises and economic organisations demonstrate that the aim of digital attacks is not only to disrupt functioning systems, but also to weaken economic resilience and obtain strategically important information.

At the same time, the existing international mechanisms for counteracting economic cyber-espionage are insufficient. The absence of universally recognised international rules, the difficulty of reliably attributing cyber attacks, and the limitations of interstate co-operation all significantly reduce the effectiveness of legal and diplomatic responses. Economic cyber-espionage continues to exist within a partially regulated sphere of international relations, enabling states and associated actors to exploit legal loopholes.

Effective protection against economic cyber-espionage requires a comprehensive approach combining technological, institutional, economic and legal measures. Key areas of focus include strengthening international cybersecurity co-operation, establishing common standards of cyber responsibility, improving mechanisms for protecting intellectual property in the digital environment, fostering public-private partnerships, and incorporating cybersecurity principles into national economic development strategies.

Therefore, economic cyber-espionage should be considered not only a cybersecurity issue, but also a fundamental challenge to sustainable economic development, technological independence and global economic stability.

References:

Fidler, D. P. (2013). Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies. *ASIL Insights*, 17(10). https://www.asil.org/insights

World Economic Forum. (2025). *Global Cybersecurity Outlook 2025*. Geneva: World Economic Forum. https://www.weforum.org

IBM Security. (2024). *Cost of a Data Breach Report 2024*. IBM Security. https://www.ibm.com/security/data-breach

European Union Agency for Cybersecurity (ENISA). (2024). *ENISA Threat Landscape 2024*. Athens: ENISA. https://www.enisa.europa.eu

OECD. (2023). *Digital Security and the Role of Cybersecurity in Economic Resilience*. Paris: OECD Publishing. https://www.oecd.org

Kshetri, N. (2021). Cybercrime and Cybersecurity in the Global South. *Journal of Global Information Technology Management*, 24(3), 147–150. https://doi.org/10.1080/1097198X.2021.1948881

Nye, J. S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security*, 41(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge: Harvard University Press.

Microsoft. (2024). *Microsoft Digital Defense Report 2024*. Microsoft Threat Intelligence. https://www.microsoft.com/security

Google Cloud Security. (2025). *Advanced Persistent Threats (APTs): Threat Intelligence Report*. https://cloud.google.com/security

Cavelty, M. D. (2018). Cybersecurity and the Problem of Political Order. *Global Affairs*, 4(4–5), 379–387. https://doi.org/10.1080/23340460.2018.1531123

Lindsay, J. R. (2015). Tipping the Scales: The Attribution Problem and the Feasibility of Deterring Cyberattacks. *Journal of Cybersecurity*, 1(1), 53–67. https://doi.org/10.1093/cybsec/tyv003

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, 38(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382

Clarke, R. A., & Knake, R. K. (2019). *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. New York: Penguin Press.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press.

Nye, J. S. (2011). Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly*, 5(4), 18–38.

Kello, L. (2017). *The Virtual Weapon and International Order*. New Haven: Yale University Press.

Lewis, J. A. (2023). *Cybersecurity and Cyber Conflict: Trends and Implications*. Washington, DC: Center for Strategic and International Studies.

United Nations. (2021). *Final Substantive Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.* New York: United Nations.

World Intellectual Property Organization (WIPO). (2023). *Intellectual Property and the Digital Economy.* Geneva: WIPO.

European Commission. (2023). *Cybersecurity Strategy of the European Union*. Brussels: European Commission.

Shkuta, O., Blaga, A., & Lisnichenko, D. (2025). Role and place of the State Bureau of investigation as a entity of preventing economic crime in the conditions of martial law in Ukraine. *Baltic Journal of Economic Studies*, 11(4), 400–404. https://doi.org/10.30525/2256-0742/2025-11-4-400-404

State Service of Special Communications and Information Protection of Ukraine. (2024). *Report on Cyber Threats in Ukraine*. Kyiv.

Ministry of Digital Transformation of Ukraine. (2024). *Strategic Directions for Cybersecurity Development in Ukraine*. Kyiv.

Cybersecurity Ventures. (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine.

Cybersecurity Ventures. (2024). Cybercrime To Cost The World $9.5 Trillion Annually in 2024. Cybercrime Magazine.

Cybersecurity Ventures. (2025). Official Cybercrime Report 2025. Cybercrime Magazine.

Cybersecurity Ventures. (2021). Global Cybersecurity Spending To Exceed $1.75 Trillion From 2021–2025. Cybercrime Magazine.

Gartner. (2024). Gartner Forecasts Global Information Security Spending to Grow 15% in 2025. Stamford, CT: Gartner.

Gartner. (2025). Forecast: Information Security, Worldwide, 2023–2029, 2Q25 Update. Gartner.

European Commission. (2025). Digital Decade 2025: Country Reports. Brussels: European Commission.