

Public policy of cybersecurity in Ukraine

Vira HAPONENKO,

Kyiv National Economic University named after Vadim Hetman, Kyiv, Ukraine

haponenko.vira@kneu.edu.ua

Abstract

Objectives: Government and civil sector activities for supporting the cyber security during the full-scale invasion in Ukraine to rethink innovative national technologies and the latest achievements in AI, in the context of Ukrainian institutional capacity and supporting informational resilience in times of crisis. **Prior work:** The research summarizes Google's report on the Munich Security Conference (2026), the official statistics on AI use in government services, a few cases of cyber-attack in Ukraine. **Approach:** Cyber security analyzed as a part of informational resilience and institutional capacity in preventing informational threats using official regulation, government strategy, business and society impact to disinformation counteraction. **Results:** The effectiveness of public policy in cyber security depends on institutional forms of state-business partnership, in particular cyber security clusters. As the networks of government, private, scientific and educational organizations they can concentrate resources, knowledge and technologies for innovative and decisions to respond quickly for informational and digital threats by society consolidation. **Implications:** Ukrainian experience in cyber security in times of crisis can be useful for both researchers and policy makers as the outputs for deepening theoretical analysis and developing public strategies and policies in shaping, preventing and managing modern informational threats. **Value:** The paper summarizes recent policies and cases of cyber security in a systematic, institutional form, including the government, public and private sectors partnership.

Keywords: public policy, cyber security, informational resilience, institutional capacity, state-business partnership, information threats.

1. Introduction (Main text)

The Ukrainian society is an active user of digital and AI tools. After 2022, the role of online government apps increased, becoming an effective method of citizen participation (electronic petitions, polls, feedback on state decisions, discussions about legislation projects), and of government services (civil status, documents, tax reports, etc.). The development of AI tools in state-civil-business partnerships seems to be a basis for democratic resilience in the condition of war restrictions.

At the same time, Ukraine faced numerous informational threats in wartime, including propaganda, fake sharing, cyber-attacks, which decreased the legitimacy of state institutions, citizens' distrust and disappointment in democratic participation opportunities. It underlines the importance of advanced and independent national methods for cybersecurity and data protection.

The research aims to rethink innovative national technologies and the latest achievements in AI, including the DIIA AI assistant, the sovereign language model (Gemma) and infrastructure, automatic check cloud services, in the context of Ukrainian institutional capacity and supporting informational resilience in times of crisis.

2. Research methodology

The main research approach is the neo-institutionalism theory and the concept of institutional capacity. The author of the paper promotes the idea about necessity of institutional shaping of cybersecurity public policy to achieve systematic, effective and stable results.

Conceptualizing the main terms of the research, the cybersecurity is understood as an element of informational security, which includes not just a digital instruments of data protection, but also developing principles of ethical AI use and critical thinking.

The principles of crisis management is used to rethink cybersecurity policy in wartime and strengthen the resilience of informational space.

The research based on content analysis of EU directives, Ukrainian legal regulations and the latest government decisions in the field of cybersecurity, summarizes Google's report on the Munich Security Conference (2026), the official statistics on AI use in government services.

The case study of cyberattack and AI implementation in Ukraine, in particular, law reforms, technical data security control and new standards of cryptographic protection (Kupyna), electronic signature checks, is used to highlight the specific practices of cybersecurity public policy, its prospects and challenges.

GenAI tools was used for visualization (ChatGPT, Notebook), translation and grammar correction (Grammarly).

3. Literature review.

Cybersecurity public policy has become one of the central areas of contemporary research due to increasing dependence on digital infrastructure, growing cyber threats, and the expansion of AI technologies [1-2].

Previous researches offer numerous concepts of cybersecurity as a governance challenge requiring institutional coordination and strategic policymaking. They highlight that cybersecurity is not merely as a technical challenge but as a multidimensional governance problem involving institutions, regulation, resilience, and public administration. Our research supports the idea that cybersecurity policy evolved from technical protection mechanisms toward strategic governance systems. It was useful for the research to analyze the proceedings of the previous SCIC. They proposed many similar definitions.

Latest studies show the specific indicators of modern cybersecurity policy, in particular integration into broader digital governance strategies, public-private partnerships, citizen engagement, data governance, and institutional digitalization increasingly shape cybersecurity policy implementation [3].

For example, Oleksandr Tsaruk and Maria Korniiets [4] argue that modern cyber threats should be understood through the concept of hybrid threats, where cyber operations are combined with political, military, economic, and information instruments.

Research by Claudiu Codreanu [5] is very close to this one. It examines Ukraine's digital governance system during wartime through the case of the government platform Diia. Codreanu argues that Ukraine provides a unique example of maintaining large-scale e-government systems despite continuous cyberattacks and military operations. His work identifies cybersecurity integration into digital governance as essential for preserving state functionality during crises. The study emphasizes international cooperation, institutional flexibility, and cybersecurity-by-design approaches.

Research conducted by Nataliia Fedirko [6] also made a great contribution to the discussed problem. It proved that digital governance mechanisms can significantly improve institutional resilience and economic recovery in Ukraine. Her work emphasizes that cybersecurity becomes a foundational component of post-war governance modernization and European integration processes.

4. Results.

4.1. Main factors of cyber security public policy development in Ukraine

Ukraine has established numerous laws about informational space protection since the early 90s. The term "cybersecurity" was regulated in 2017.

European integration strategy in Ukraine supports the development of cybersecurity policy. EU directives and regulations in cybersecurity and data protection play a fundamental role in shaping it. The NIS Directive (Network and Information Systems Directive) sets minimum cybersecurity standards for EU Member States, defines the responsibilities of operators of critical infrastructure and digital services, and establishes mechanisms for the exchanging information on incidents and coordination between national authorities. This directive aims to increase the resilience of key systems against cyberattacks and ensure the continuity of critical services, which are the basis for the functioning of the economy and public administration [7].

The GDPR (General Data Protection Regulation) [8] establishes uniform rules for the protection of personal data of EU citizens, defines the rights of users to control their own information and obliges organizations to implement comprehensive data security mechanisms. The GDPR provides an increased level of transparency in the collection, processing and storage of information, and also provides for strict sanctions for violations, which stimulates states and businesses to properly manage data.

The war totally increased the role and number of digital communications and services. Due to the mass migrant and refugees flows, displaced persons, destroyed properties people often have no access to the public services in person or paper documents.

At the same time, it was observed a total increase of cyber attacks on government sector from 2022 (see fig.1.) [9]

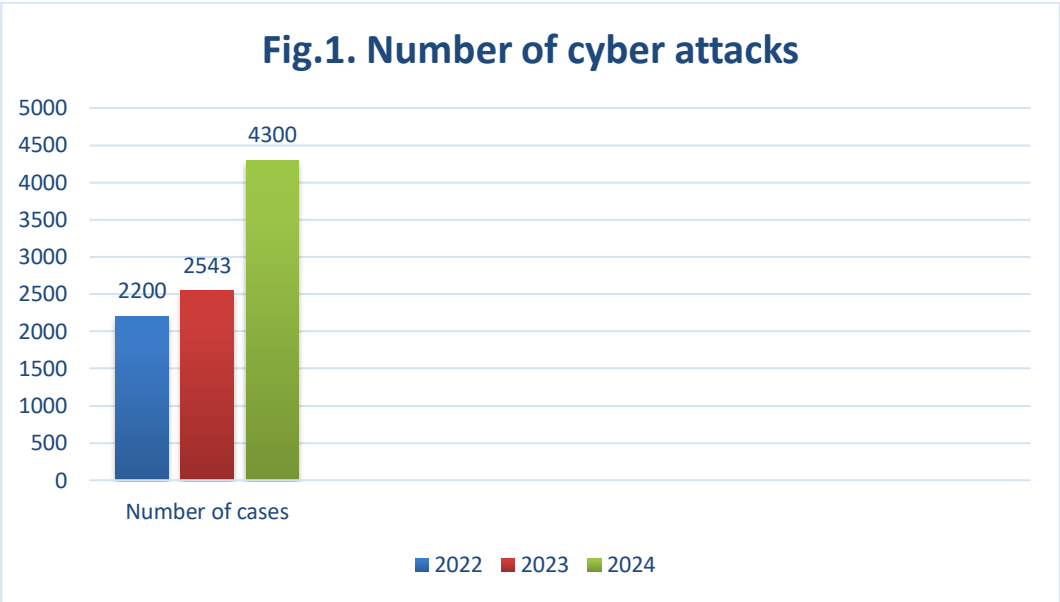


Fig.1. Source: cert.gov.ua

The largest cyberattack on Ukraine's state registers took place on December 19, 2024, when a targeted strike by Russian special services temporarily paralyzed the operations of key databases administered by the Ministry of Justice of Ukraine. This incident became one of the most serious challenges for Ukraine's digital infrastructure, as it blocked the implementation of basic legal and property transactions for several weeks [10].

On December 12, 2023, hackers attacked the core of the Kyivstar network. They managed to do this by hacking the account of one of the company's partners. About 24 million subscribers were left without communication. The attack on the virtual infrastructure was successful. Despite the fact that the network was completely turned off, the hackers managed to destroy 40% of the infrastructure. For the hack, the attackers used the Mimikatz stealer, which collects information on the victim's computer and transfers it to the hackers [11].

It shows that, despite the institutional guarantees of cybersecurity, this area requires new crisis management approaches. Such cases performs that cybersecurity policy isn't only the protection against threats, but also a value-ideological function. It ensures the preservation of national identity, the consolidation of society and trust to the state. It is through the information environment that a common system of values is formed, the perception of the enemy and the ally is determined, and therefore, the internal unity of the nation is maintained.

4.2. Peculiarities of cybersecurity institutional system in Ukraine

The crucial risks for cybersecurity in wartime required a systematic and consolidated institutional base. The institutional mechanism for ensuring cybersecurity in Ukraine constitutes a holistic system of state authorities that coordinate, regulate and monitor the information and digital space.

Thus, the interaction between cybersecurity public institutions should be carried out on the basis of the principles of coherence, subordination and interdepartmental coordination. Such a comprehensive approach to cybersecurity policy aims to combine the efforts of political, security, technical and media institutions to create an effective cybersecurity system capable of adapting to the new challenges of the digital age.

The contemporary structure of the cybersecurity institutional system in Ukraine illustrated in the Fig. 2.

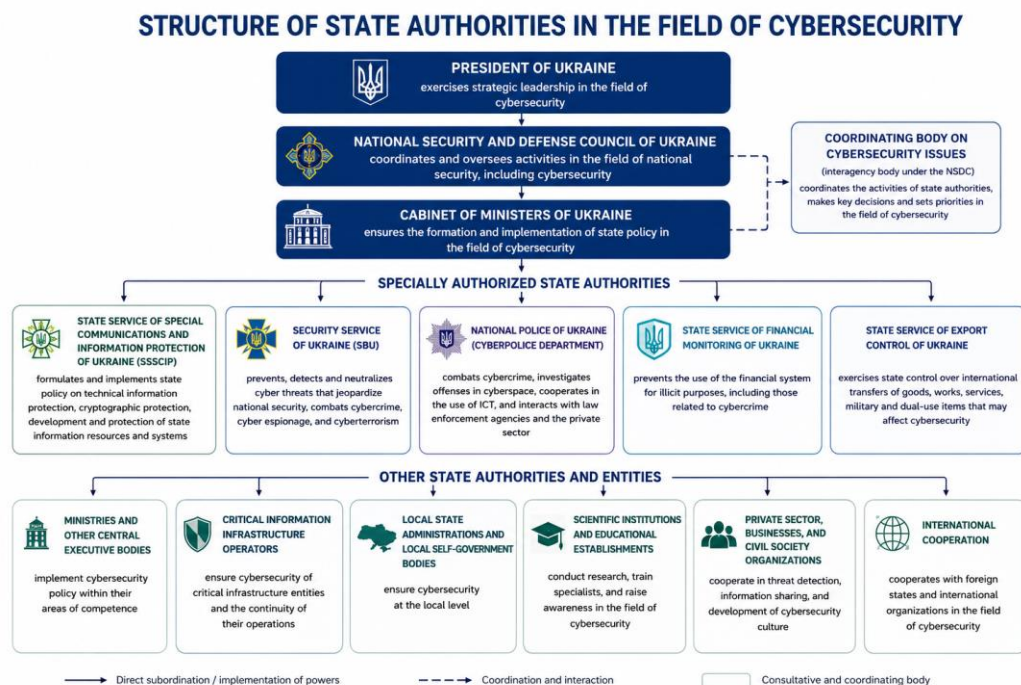


Fig 2. Cybersecurity institutional system in Ukraine. Generated by ChatGPT.

4.2.1. Government institutions of cyber security in Ukraine

The central role of the state institution can be explained by necessity not just to establish roles and guarantees of cybersecurity, but also as a coordinator of interaction between authorities, the media, civil society and international partners. In this context, cybersecurity becomes a tool of political management, which allows ensuring the legitimacy of power, neutralizing destructive information influences and maintaining a communication balance in society.

The central place in this system belongs to the National Security and Defense Council of Ukraine. It determines the main directions of state policy in the field of information and cybersecurity, coordinates the activities of other executive bodies, and approves relevant strategies and programs. The NSDC acts as a strategic decision-making center related to the protection of the state's information sovereignty, particularly in the context of military aggression and hybrid threats.

An important role is played by the Security Service of Ukraine, which is tasked with identifying, preventing and neutralizing information and cyber threats that encroach on the constitutional order, state secrets and the stability of society. The SSU conducts counterintelligence measures, investigates cases of information sabotage, and also participates in the formation of a regulatory framework on information security issues.

In 2019, the Ministry of Digital Transformation was founded. It develops digital governance and services, projects such as DIIA, protects state digital sources.

The National Council of Ukraine on Television and Radio Broadcasting carries out regulatory activities in the media space, monitoring compliance with legislation on information, freedom of speech, preventing the spread of propaganda and hate speech.

To the institutional system of cybersecurity policy, we also can add the Ministry of Defense of Ukraine, the State Service for Special Communications and Information Protection (SSCI), the Ministry of Culture and Information Policy, and the Ministry of Internal Affairs, while some aspects of their activities also include cyber protection of military information systems, monitoring information campaigns and information counteraction to hostile influences.

4.2.2. Non-government institutions of cyber security

Public-Private Partnership is a necessary condition for creating effective mechanisms for monitoring, preventing and responding to cyber attacks. That is why the involvement of the private sector, primarily IT companies, telecommunications operators and software developers, becomes a necessary condition for the formation of a sustainable information security system.

In today's cyberwarfare environment, private IT companies are often the first targets of cyberattacks, as they ensure the functioning of critical digital services, cloud platforms, payment systems, and information resources of government agencies. Attacks on the private sector have not only economic but also strategic consequences, as they can disrupt of government services, leak confidential information, and destabilize social processes. In this context, private companies actually become the "first line of defense" in cyberspace, which necessitates close coordination of their actions with government agencies.

In the field of non-government cybersecurity institutions special attention should be paid to the analysis of *cybersecurity clusters* [12]. Cybersecurity clusters are network

associations of state bodies, private companies, scientific institutions and educational centers, whose activities are aimed at jointly solving problems in the field of cyber defense. The effectiveness of such clusters lies in the concentration of resources, knowledge and technologies, which allows for a quick response to new threats and the development of innovative solutions.

The practice of functioning of cybersecurity clusters demonstrates their ability to increase the level of resilience of the state's information infrastructure. Due to horizontal interaction between cluster participants, the response time to incidents is reduced, coordination of actions is improved and duplication of functions between the public and private sectors is reduced. In addition, clusters contribute to the Ukraine's integration into international cybersecurity networks, which is especially important in the context of the transnational nature of cyber attacks.

At the same time, the effectiveness of public-private partnerships and cybersecurity clusters depends on the level of trust between the state and business, the clarity of legal regulation and the availability of transparent accountability mechanisms. In the absence of proper guarantees for the protection of commercial secrets and personal data, private companies may be limited in their readiness for deep cooperation with state authorities. Therefore, the formation of legal and organizational conditions for sustainable partnership is one of the priorities of state policy in the field of information security.

Therefore, public-private partnership in the context of cyberwar is not an auxiliary, but a system-forming element of the institutional model of ensuring information security in Ukraine. The involvement of private IT companies and the development of cybersecurity clusters allow increasing the state's adaptability to modern cyber threats, ensuring more effective protection of critical infrastructure and form a comprehensive model for responding to information challenges.

The public sector can also be represented by scientific institutions and public organizations act as a sources of analytical data, expert assessments and methodological recommendations in the information security system. The academic environment forms scientific approaches to the analysis of information risks, develops new models of cyber protection, and predicts trends in the development of the information space. Public organizations, in turn, participate in educational and monitoring initiatives, contribute to raising the level of digital culture of the population, and also monitor the transparency of the actions of state institutions in the field of information policy. Their activities create the necessary balance between security and freedom of speech, preventing the potential abuse of power in the field of information control.

In addition, non-government activities are implemented through national campaigns such as "Filter" and "Media Literacy - a Shield Against Fakes". These initiatives aim at raising citizens' awareness of the methods of spreading fake news, manipulative narratives and information attacks. They include the publication of educational materials, conducting educational campaigns in the media and on social networks, as well as the creation of online

platforms for fact-checking. Thanks to such programs, the state not only responds to information threats, but also forms critical thinking and the ability to independently assess the reliability of information in society.

“Filter” is a program coordinated by the Ministry of Culture and Information Policy of Ukraine that aims not only to inform citizens about the threats of disinformation but also to form in them a responsible attitude towards information consumption. The emphasis on explaining the mechanisms of creating fakes, the role of emotional triggers and the algorithms of social networks contributes to an increase in the level of reflection on the received media content. A similar function is performed by the program “Media literacy - a shield against fakes”, which is focused on the educational component and long-term formation of critical thinking skills.

Also, it should be mentioned the contribution of International actors (European Union, NATO, the UN, the OSCE), as well as international cybersecurity organizations (the European Cybersecurity Agency ENISA). Their participation consists in the establishment of common standards, information exchange, joint exercises, financial and technical support for national security programs. Ukraine's cooperation with these institutions contributes to integration into the European security space and increasing the level of compatibility with Western response systems.

So international cooperation is an integral element of the information security strategy of Ukraine. It provides access to advanced technologies, expertise, and coordination mechanisms. In particular, cooperation with NATO allows integrating Ukrainian cyber defense standards into Euro-Atlantic norms, receiving technical support and participating in joint cyber defense exercises. Participation in EU programs contributes to the harmonization of national legislation with the European legal framework, and partnership with ENISA expands opportunities for incident analysis and the implementation of modern methods of information risk management.

4.3. The latest achievements in public policy in cyber security in Ukraine.

The war actions in Ukraine became a strong stimulant for developing cybersecurity national policies and systems. Many startups take place in defence tech. Best AI instruments are implemented for protection from military attack.

Among the innovations being implemented in Ukraine are the first national AI agent (AI assistant “Diya.AI”), which provides public services and works on the Gemini model; a national language model based on Gemma, thanks to which Ukraine will be able to deploy the model on its own sovereign infrastructure, while maintaining full control over data; cloud technologies that create conditions for automatic system verification, etc. [13].

The transition to the new cryptographic protection standard "Kupyna" took place on February 10, 2026, which will help strengthen the resistance of qualified electronic

signature (QES) keys and digital data to modern cyberthreats using a new enhanced algorithm [14].

In September 2025, the Ministry of Digital and Google announced a new stage of cooperation on using the company's AI technologies to develop government AI products in Ukraine. Ukraine is currently among the top five global leaders in the digitalization of public services. With the assistance of the Digitization for Growth, Integrity and Transparency (UK DIGIT) project and the support of the Swiss-Ukrainian EGAP Program implemented by the Eastern Europe Foundation, Ukraine plans to provide public services on the Diia.AI portal, built on the Gemini 2.0 Flash model and deployed on the Vertex AI cloud platform. The AI assistant is currently in open beta testing mode to provide personalized consultations and services [15].

A lot of reforms became possible because of financial support. For example, Funding for the systemic development of Ukraine's digital security is provided through the U.S. Civilian Research & Development Foundation (CRDF Global), which has significant experience in implementing effective cyber deterrence mechanisms and implementing technical assistance projects in Ukraine. Canada's support within the Tallinn Mechanism is a strategically important step in combining international and interregional experience, which strengthens the state's ability to counter cyber threats, protect civilian infrastructure, and ensure the resilience of digital processes.

5. Conclusions

Today, cybersecurity is not only the protection of resources, but a dynamic political system of interaction in which the state, media and society jointly shape the nation's resilience to information challenges. Ukraine creates an integrative model that is the key to Ukraine's information sovereignty in the conditions of hybrid warfare and global digital competition.

Summarising the results of the paper, we highlight that cybersecurity public policy in Ukraine has a strong legal institutional framework, appropriate to the EU and global trends. It is developed dynamically to adapt for the war challenges and threats. Today's capacity of cybersecurity policy lies in the consolidated efforts of the public and private sectors, a combination of international founding programs and national innovative programs of digital tools.

Military conditions determine multi-structural directions of cybersecurity public policy, including digital and data protection, counteracting propaganda and disinformation, supporting society's resilience to informational threats, providing roles for ethical AI use and responsible information sharing, shaping people's critical thinking and media literacy.

References:

- [1] G., Boce, & B., Kanushi, "ChatGPT's Influence on Cybersecurity: Reduce and Understanding the Risks". SCRD Preprints. Vol. 2, 1, 2025
- [2] A., Hyra, & F., Premti, "*The Double-Edged Sword of AI in Cybersecurity*". SCRD Preprints. Vol. 1, 1, 2024

- [3] K. . Pashaj, V. . Tomço, and E. . Gjika, “From threat to response: The evolution of cybersecurity in Albania”, *SCRD-PP*, vol. 2, no. 1, Jun. 2025, Accessed: Jun. 01, 2026. [Online]. Available: <https://www.scrd.eu/index.php/scrdd-pp/article/view/646>
- [4] O. TSARUK and M. KORNIETS, “Hybrid nature of modern threats for cybersecurity and information security”, *SCRD*, vol. 4, no. 1, pp. 57–78, Mar. 2020, doi: [10.25019/scrdd.v4i1.63](https://doi.org/10.25019/scrdd.v4i1.63).
- [5] C. CODREANU, “Developing e-government under cyber threats and Russia’s war: Ukraine’s Diia platform”, *SCIC*, vol. 12, pp. 429–437, Sep. 2025, Accessed: Jun. 01, 2026. [Online]. Available: <https://www.scrd.eu/index.php/scic/article/view/709>
- [6] N. FEDIRKO, “Leveraging smart governance for Ukraine’s macroeconomic recovery and stabilisation”, *SCRD*, vol. 10, no. 1, pp. 109–128, Feb. 2026, doi: [10.25019/hpnjx94](https://doi.org/10.25019/hpnjx94).
- [7] NIS2 Directive: securing network and information systems. <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>
- [8] General Data Protection Regulation. <https://gdpr-info.eu/>
- [9] Cybersecurity Threat Landscape of Ukraine in 2023. https://understandingcyberwar.org/wp-content/uploads/2024/09/Proekt_3_en.pdf
- [10] Information threats of modernity and socio-political mechanisms for their elimination [Electronic resource]: collection of the International Round Table, November 6, 2025; Kyiv: KNEU, 2026. 140 p. <https://ir.kneu.edu.ua/handle/2010/53900>
- [11] O, Koval, “What was the hacker attack on Kyivstar and how was the company restored?” March 19, 2024. <https://dou.ua/lenta/news/kyivstar-cyber-attack-restoration/>
- [12] National cybersecurity clusters. <https://cybersecuritycluster.org.ua/en/>
- [13] M., Jadotte. “How we’re helping democracies stay ahead of digital threats”. 2026. Feb. 11. <https://blog.google/innovation-and-ai/technology/safety-security/how-were-helping-democracies-stay-ahead-of-digital-threats/>
- [14] Strengthening cybersecurity: switching to a modern data encryption algorithm. 2026. Feb. 10. URL: <https://thedigital.gov.ua/news/how-tos-posyliuyemo-kiberbezpeku-perekhodymo-na-suchasnyy-alhorytm-shyfruvannia-danykh>
- [15] Tallinn Mechanism launches platform for cooperation with the private sector. <https://thedigital.gov.ua/news/technologies/tallinnsky-mekhanizm-zapustyv-platformu-dlia-spivpratsi-z-pryvatnym-sektorom>
- [16] Teaming up with global technology leaders to develop AI: how Diia.AI works on Gemini technology. <https://thedigital.gov.ua/news/technologies/obednuemosya-zi-svitovimi-tekhnogigantami-dlya-rozvitku-shi-yak-diyai-pratsyue-na-tekhnologii-gemini>