Public Policy and Accounting
ISSN 2707-9325

UDC 004.056.5:339.924(477)

Challenges and prospects for the formation of state policy in the field of cybersecurity and combating cybercrime

Savchuk Serhii[1]

Applicant
Zhytomyr State Polytechnic University

Abstract

Cyberattacks aimed at disrupting the functioning of critical infrastructure, spreading disinformation, and stealing personal data and financial resources pose significant risks to states' national security. The purpose of the study is to substantiate the challenges Ukraine faces in ensuring cybersecurity, particularly in the context of hybrid warfare, and to determine the prospects for the formation of state policy in cybersecurity and combating cybercrime. The paper highlights the main threats arising in cyberspace, their impact on society, the economy, and state institutions, and the factors ensuring counteraction to cybercrime. The main types of cyberattacks used by intruders against other states are systematized and grouped according to the relevant features. Particular attention is paid to the prospects for the formation of an effective state policy in the field of cybersecurity. The author identifies the key directions for improving the legislative framework, strengthening technical capabilities for monitoring and responding to cyber threats, and increasing the level of international cooperation and coordination with other countries and international organizations. It is proved that an effective state policy in the field of cybersecurity should be based on a comprehensive and systematic approach that takes into account both internal and external challenges and integrates the best international practices of implementing modern information security technologies.

Keywords: cyber threats; cybercrime; cyber defense; state policy; cybersecurity; hybrid warfare.

1. Introduction

In the modern era, cyberspace provides many new opportunities while simultaneously serving as a platform for the creation of global threats that have no borders. Cyberattacks have become an integral part of modern hybrid warfare. They are used to undermine state institutions, create economic pressure, destabilize society, and manipulate information. Today, it is possible to harm state institutions or critical infrastructure not only physically, but also remotely through hacker actions aimed at destroying the integrity, confidentiality, and availability of information resources.

Since 2014, russia has been actively conducting massive cyberattacks against Ukraine aimed at undermining economic stability, destroying critical infrastructure, and destabilizing society. Since the beginning of russia's full-scale invasion of Ukraine in 2022, the scale and intensity of cyber operations have increased significantly. Attacks on government institutions, the energy sector, the media, and the banking system have become a regular practice, complementing physical military action. Hackers from russia launch more than ten cyberattacks on Ukraine every day. These cyberattacks have been extremely disruptive to Ukraine's economy, with a particularly negative impact on critical infrastructure.

In 2023 alone, more than 2,500 thousand cyber incidents were recorded in Ukraine, which is 15.9% more than in 2022. According to the governmental computer emergency response organization CERT-UA, which is engaged in the prevention,

Corresponding author:
[1] ORCID: https://orcid.org/0009-0007-7436-0702
doi: https://doi.org/10.26642/ppa-2024-1(9)-30-38

detection, and response to cyberattacks and cyber incidents, more than 347 attacks were directed at local government bodies, 175 at security and defense sector organizations, and 127 attacks targeted private organizations [1]. Cyberattacks have become a virtual weapon synchronized with physical hostilities in the territory of Ukraine. Russia employs attacks on information systems, promotes a disinformation campaign in the media space, and uses spyware that not only paralyzes the work of infrastructure but also creates a negative information field among the population. Despite the challenges that Ukraine is currently facing, the country demonstrates a high level of resilience, including developing cyber defense systems, receiving support from international partners, and introducing new strategic documents at the legislative level to counter existing cyberattacks.

2. Literature review

The issues of state policy on combating cybercrime have been studied at different times by different scholars: Y.Garashchenko, D.Grytsyshen, I.Dragan, A.Didenko, I.Diorditsa, O.Zherebets, Y.Zavgorodnia, I.Kotsman, O.Kravchuk, A.Lavnyk, R.Lukianchuk, Y.Onyshchenko, O.Orlov, V.Tsymbaliuk, T.Yarovyi [2-9], etc. In his works, A.Didenko emphasizes that the country's cybersecurity is "...a special set of measures aimed at combating and preventing cyberterrorism and cybercrime, neutralizing real and potential cyber threats, organizing effective protection of the information space and domestic information resources" [4]. The scholar emphasizes that "...the activities of state bodies and public organizations in the field of combating cybercrime are focused on regulating information relations, developing effective actions to combat cybercrime, intensifying efforts to prevent cybercrime and ensuring the safe development of the information society [3]".

In addition to the perspectives mentioned above, let us consider the viewpoint of researchers O.Orlov and Yu.Onyshchenko regarding the state's managerial influence on cybersecurity. The researchers assert that "...the system of combating cybercrime is understood as the coordinated activities of state and executive authorities, organizations and enterprises of all forms of ownership in the following areas: research, analysis, and assessment of cyber threats, forms and methods of their organization, as well as the level of cybersecurity in the real conditions of informatization of the state and society; improvement of the current legislation on cybersecurity following international norms at the level of the UN, NATO, Interpol, European Union, etc.; implementation of effective measures for the prevention, investigation, and counteraction of cybercrimes; and training specialists in the field of cybersecurity and combating cybercrime" [8, 9]

The formation of the concept of "state policy of combating cybercrime" is influenced by a multidimensional understanding of state policy, which has become the basis for various approaches to the interpretation of this term. Researcher E. Young pointed out the following characteristics of state policy: "...it is an activity carried out by a governmental body that has the grounds and legislative authority to carry out such activities; it represents the state's response to real social issues, needs or problems, meaning that such a policy is designed to respond to specific problems, needs or concerns of citizens, non-governmental organizations, such as society or community; it is goal-oriented, or in other words, it aims to achieve several goals to attempt to solve particular problems, issues or needs in a given society; it is a well thought out method or strategy, not a single decision, action or reaction; it is a decision to take some action or conversely, to refrain from action, meaning that the defined policy strategy may lead to actions that will try to solve an issue, or it is based on the belief that the current policy will solve an issue, i.e. no action will be taken; it is implemented by one or a group of actors, in other words, the policy can be implemented by a government representative or a public body or by many participants; it provides reasonable grounds for action, i.e., as a rule, it contains logical explanations on which it is based; it is not an intention or a promise, it is a decision already made [10, p. 6]".

While acknowledging the achievements of both domestic and foreign scholars, it should be noted that the research conducted so far is fragmented and lacks a systematic approach to mastering this topic. This indicates the need to develop key provisions of state policy in cybersecurity and combating cybercrime.

3. Identification of previously unresolved issues and formulation of research hypotheses

Developing an effective state policy in cybersecurity and combating cybercrime requires an integrated approach that considers both technical and social, economic, and legal aspects. The main challenges are the rapid evolution of cyber threats, insufficient human resources, low public awareness, and the need for international cooperation. Policy perspectives include the establishment of national cybersecurity centers, the development of specialized educational programs, improving inter-agency and international cooperation, and enhancing the legislative framework to respond to new challenges effectively. The above factors determine the need for a comprehensive approach to developing state policy in cybersecurity and combating cybercrime.

4. Methodology and research methods

The study was carried out according to a general methodological framework using an integrated and systematic approach based on statistical and economic analysis methods to assess global and national trends in cybercrime and information security threats, as well as the analytical dimension of cybersecurity and cybercrime in the global space and the consequences of cyber threats and Russia's cyberwar against Ukraine. The methods of strategizing, analogy, systematization, structuring, analysis and

synthesis, induction, and deduction were used to assess the challenges and formulate prospects for developing state policy in cybersecurity and combating cybercrime.

5. Main results

The Cybersecurity Strategy of Ukraine states that "...russia remains one of the main sources of threats to national and international cybersecurity, actively implementing the concept of information confrontation based on a combination of destructive actions in cyberspace and information and psychological operations, the mechanisms of which are actively used in the hybrid war against Ukraine. Such destructive activity creates a real threat of cyber terrorism and cyber sabotage against the national information infrastructure" [11].

Modern cyberattacks are becoming increasingly sophisticated and dangerous, posing serious threats to critical infrastructure. Hackers are focusing on identifying vulnerabilities in control systems and employing innovative tools, including multi-functional malware, ransomware, botnets for distributed denial-of-service (DDoS), and interference with cloud services and production systems through supply chains. Given the development of artificial intelligence, the scale and impact of such threats may increase significantly in the next 5-10 years, creating new challenges for global cybersecurity.

The main types of cyberattacks used by attackers against other states are destructive attacks, subversive attacks, data mining, and disinformation. The definitions of these types of attacks are as follows:

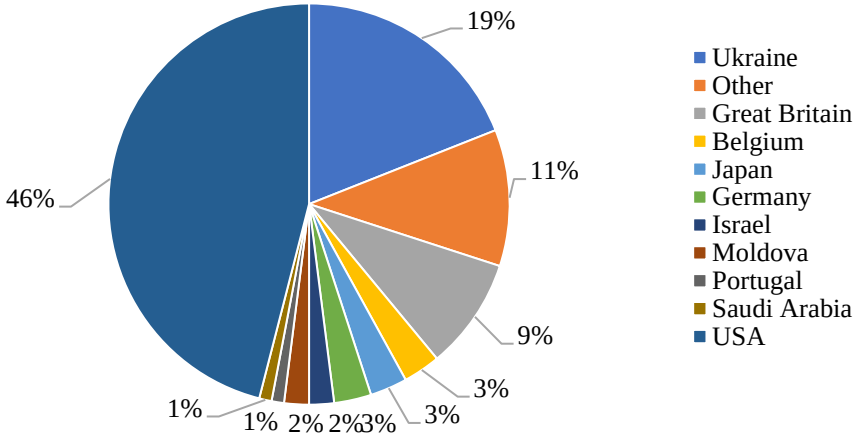
- destructive attacks are cyberattacks aimed at permanently deleting data or damaging systems in such a way that they cannot be recovered. Such attacks can have long-lasting effects on organizations, especially if they do not have access to backups or the ability to restore systems. An example is the use of data destruction malware targeting Ukrainian government agencies and other important sectors [12];

- subversive attacks are cyberattacks aimed at destabilizing services and disrupting operations. They occurred during the conflict, in particular against Ukrainian organizations in the initial stages of the invasion, as well as against government agencies in some NATO countries in connection with announcements of threats to public security or the economy. The most common type of such attacks was distributed denial-of-service (DDoS), which particularly affected the public and financial sectors [12];

- data-mining - cyberattacks that result in the theft or leakage of data or the acquisition of data for espionage, surveillance, or reconnaissance purposes. While the latter are expected activities in cyberspace in the context of war and geopolitics, the former are attacks that are actively carried out by collectives of actors in the name of activism. Data related to private and public organizations is being stolen and published online at an unprecedented rate. Data has become a weapon in hacking and leakage operations [12];

- disinformation - information operations based on disinformation and propaganda are not new methods of warfare, but cyberspace has allowed them to be deployed at an unprecedented speed and scale. Attacks aimed at spreading false information and propaganda have become a characteristic feature of this armed conflict. From SMS spam spreading false information about ATM technical malfunctions to cyberattacks on TV channels, in which false information is displayed in the news feed or in-broadcast, as well as fake videos, and attackers hacking into email accounts to access the social media accounts of high-ranking Ukrainians to post disinformation [13].

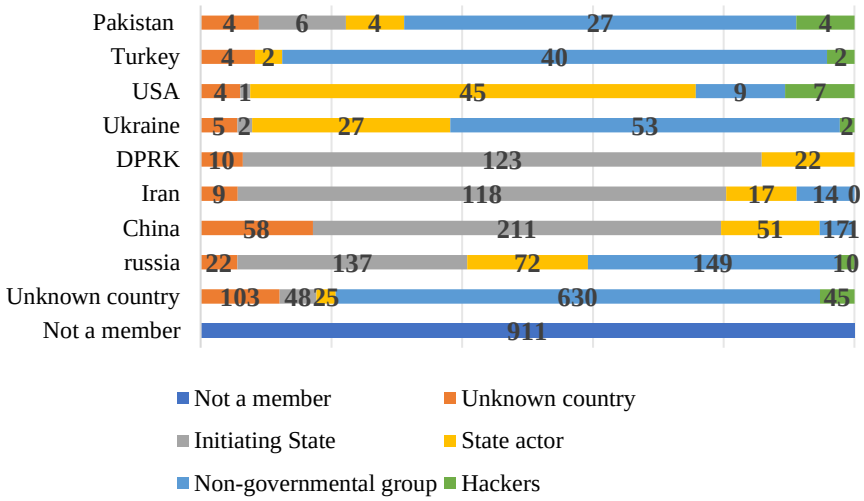
Globally, more than 200,000 attacks were carried out every week in 2021, with Ukraine's share among the countries under attack at about 19% (Fig. 1). The United States ranks first with a share of more than 46% of all incidents.



Source: compiled by the author based on [13]

Fig. 1. Geographical distribution of cyberattacks in the world, 2020-2021

Among the most popular countries that initiate politically motivated cyberattacks are China and russia, with more than 295 and 288 attacks against other countries in 2000-2023. Iran is in second place with more than 131 motivated attacks. In the period from July 2023 to June 2024, approximately 33% of recorded network intrusions by russian state or affiliated cyber threat actors targeted government entities. Additionally, 15% of attacks targeted think tanks and NGOs. Furthermore, russian state actors directed 9 per cent of cyberattacks at educational institutions in other countries, according to the conducted research (Figure. 2).



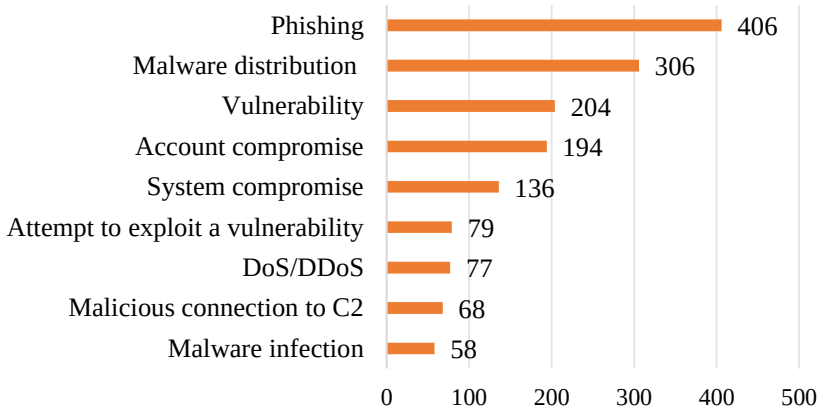
Source: compiled by the author based on [13]

Fig. 2. Countries-initiators of politically motivated cyberattacks, 2000-2023

It should be noted that cybercriminals use a wide range of methods to gain initial access to their targets. The main approaches include phishing campaigns, exploiting unpatched vulnerabilities in on-premises Exchange servers, and compromising IT vendors. These methods often serve as a critical entry point for subsequent operations, such as data destruction, theft, and prolonged access or surveillance. To avoid detection, attackers constantly modify their malware, adapting it for each new attack. Microsoft's report focuses on attacks using “wiper” malware. The name “wiper” reflects its primary function - the complete erasure of data from the victim's hard drive, resulting in irreversible loss of information. This makes such attacks extremely dangerous for organizations that target them [12].

According to Microsoft, Russian-linked criminal groups were used for attacks in Ukraine as early as March 2021. These groups carried out periodic assaults, causing harm to organizations both within Ukraine and among its allies. Microsoft identified the following russian cyber groups, tracked long before the invasion: Actinium, Nobelium, Bromine, Seaborgium, and dev-0257. These groups sought permanent access to their specific interests, including Ukraine's defense sector, defense-industrial base, foreign policy, national and local administration, law enforcement, and humanitarian organizations [12]. Although Microsoft has refrained from drawing definitive conclusions about the level of coordination between these groups, their joint activities aim to maintain continuous access to systems for gathering strategic and operational intelligence. Moreover, their actions potentially lay the groundwork for future destructive attacks against Ukraine amid the ongoing war [12].

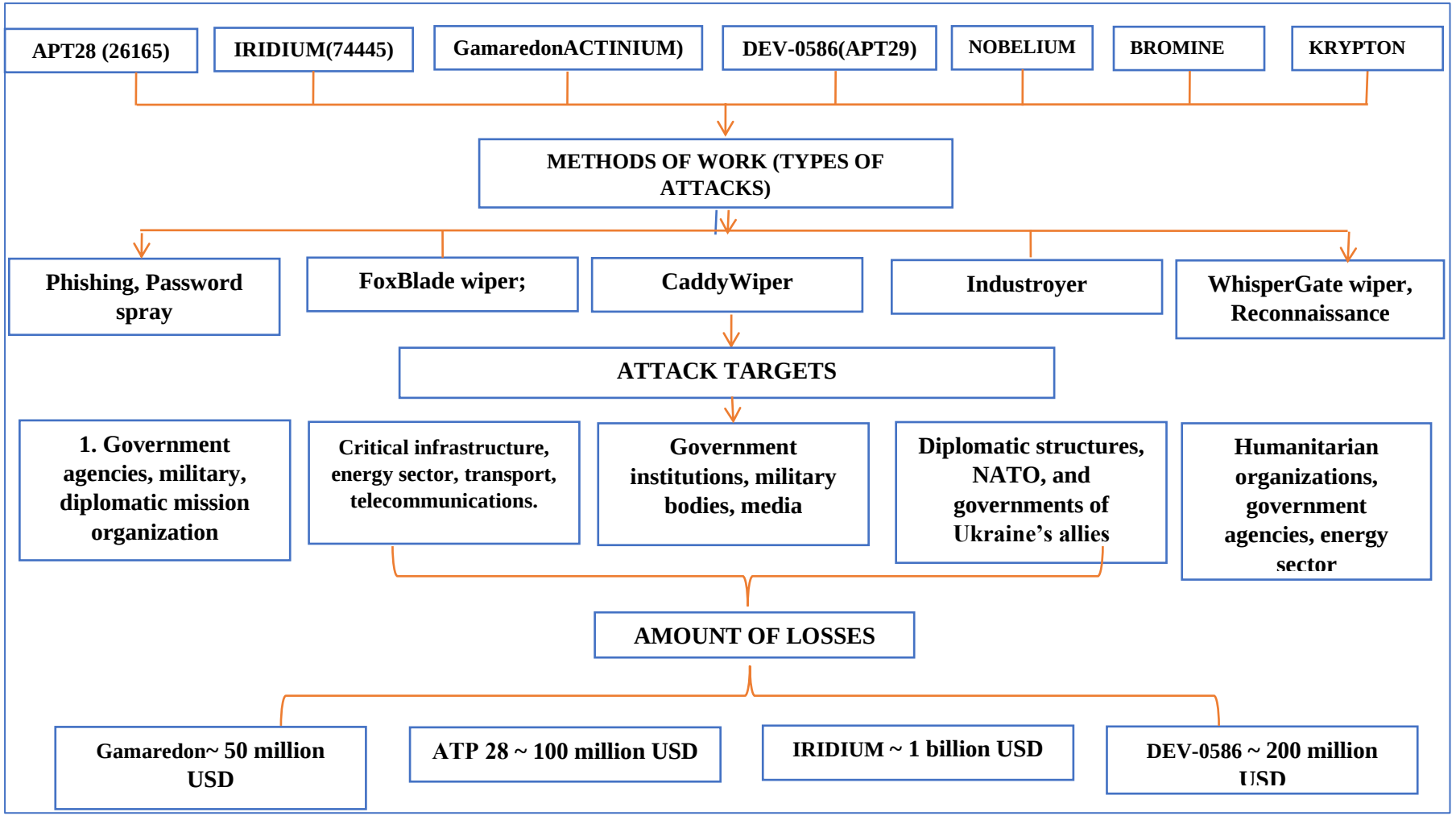
The day before the military invasion on February 24, 2022, operators linked to the GRU (russian military intelligence) carried out disruptive attacks on hundreds of systems of the Ukrainian government, IT sector, energy, and financial organizations. The activities observed by Microsoft included attempts to destroy, disrupt, or infiltrate the networks of government agencies and critical infrastructure. Some of these targets were simultaneously subjected to ground assaults and missile strikes by russian armed forces. These network operations were intended not only to impair the functions of the targeted institutions, but also to prevent citizens from accessing reliable information and vital services, and to undermine trust in the country's leadership [12].



Source: compiled by the author based on [13]

Fig. 3. Number of Russian cyberattacks against Ukraine by type, 2023

It should be emphasized that in 2022, the following areas were massively exposed to cyberattacks (Figure. 3): public administration - 132 attacks, the financial sector - 63 attacks, media - 61 attacks, ICT (Information and Communication Technologies) - 59 cases, and energy facilities - 31 incidents.

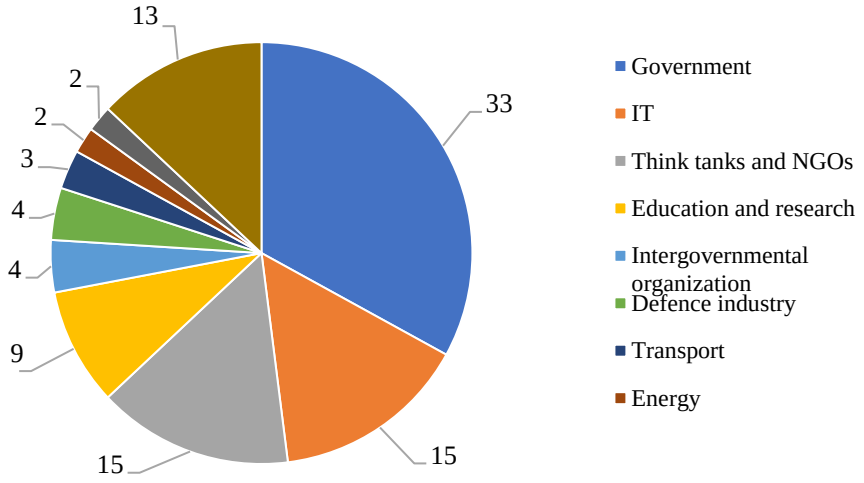


Source: compiled by the author based on [14]

Fig. 4. Major russian cyber groups: methods, goals and estimated losses in 2021-2022

According to Ukrenergo, in 2022, the number of attacks on Ukraine's energy sector increased by 20–25%. The most common attacks were DDoS, phishing, and attempts to execute malicious code. The most intense period of cyberattacks was recorded in March 2022, when Ukraine was connecting to the EU's energy system [149]. In the first half of 2023, the most notable tactic used by attackers to cause cyber incidents was phishing, with over 406 recorded cases. This marks a significant difference, as malicious software distribution dominated in the first and second halves 2022. A particularly harmful trend is the targeting of Ukrainian non-profit organizations, which are a vulnerable target due to their general lack of preparedness and absence of resilience measures (see Fig. 4).

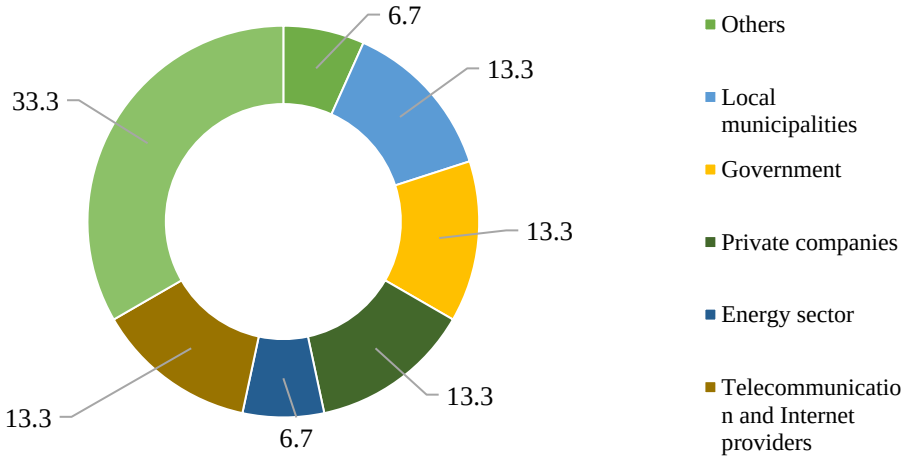
In 2023, employees of the Main Intelligence Directorate (GRU) and the federal security service (FSB) of the russian federation were involved in various cyberattacks. For instance, in the first half of 2023, military intelligence teams identified as UAC-0056 (Ember Bear), UAC-0028 (APT28), and UAC-0082 (Sandworm) carried out over 50 dangerous attacks, with GRU representatives responsible for approximately 11 incidents of critical or high severity. From July 2023 to June 2024, the primary targets for the russian federation, among other countries worldwide, including Ukraine, remain government entities, accounting for over 33% of attacks. The IT sector, think tanks and non-governmental organizations are the second most targeted, representing over 15%. The education sector accounts for more than 9% of cybercrimes committed by russian groups (see Fig. 5).



Source: compiled by the author based on [15]

Fig. 5. Targets of russian cyberattacks against other countries, including Ukraine, from July 2023 to June 2024

Among the Ukrainian sectors in 2023, mass media became one of the key and relevant targets for military hackers under the control of the main intelligence directorate of the ministry of defense of the russian federation. Although the media are purely civilian objects, they hold strategic significance for the russian command, which views them as essential to military and informational operations. As a result, the media remain under constant scrutiny from russian hackers who use them to carry out influence operations. The use of hacking attacks is complemented by other forms of aggression, such as propaganda, missile strikes, and drone attacks on critical energy infrastructure and agricultural export routes. According to this approach, military hackers direct a significant portion of their attacks at crucial civilian services, including the media, communication networks, and the public sector. This underscores the systemic nature of the russian strategy aimed at undermining stability and destabilizing key sectors of society (Fig. 6).



Source: compiled by the author based on [15]

Fig. 6. Distribution of cyberattacks committed by russia against Ukraine by sector, 2023

The energy sector is vital for ensuring the functioning of critical and civilian infrastructure in Ukraine. Hackers repeatedly attempt to launch attacks on energy facilities using a multi-stage influence tactic: power outages, destruction of substation control, destruction of intermediate telecommunications substations (modems), destruction of workstations, and destruction of server equipment. The complexity of attacks on the energy sector has significantly increased because hackers know that these networks and companies (since 2014) have a similar structure and common vulnerabilities or advanced protection practices. This has allowed them to prepare operations better. Unfortunately, IT teams at these facilities do not always have the expertise or resources to detect and counteract these threats.

When detecting cyberattacks, several problems hinder countermeasures and effectively eliminate their consequences. Among them are the following:

- *insufficient level of awareness and staff training.* Employees who lack sufficient knowledge in the field of cybersecurity may fail to recognize signs of a cyberattack, such as phishing emails or system behavior anomalies. The lack of regular training and drills leads to situations where even simple attacks, such as social engineering, go unnoticed. Poor preparation of cybersecurity specialists can complicate the incident response process;
- *high level of attack complexity.* Attackers choose advanced methods such as APT (Advanced Persistent Threat), which involve prolonged preparation, sophisticated tools, and disguising as legitimate activity;
- *there is a large volume of data to analyze.* Modern information systems generate many logs and events, making analysis labor-intensive and time-consuming. Automated systems often produce false positives, complicating the detection of real threats. A lack of resources to process such a volume of information reduces the effectiveness of analysts;
- *lack of practical monitoring tools.* Outdated software may be ineffective against modern cyber threats. The lack of integration between systems (e.g., SIEM, antivirus, IDS/IPS) complicates complete incident analysis. There is a shortage of modern AI-based solutions for automation anomaly detection;
- *complexity of internal threats.* Insiders may use their access rights to carry out malicious actions that are difficult to distinguish from legitimate activity;
- *lack of continuous monitoring of user actions in the system.* Insider forecasts often go unnoticed due to a low level of trust in employees;
- *the speed of changes in threats*. New attack methods constantly emerge, requiring continuous security systems and signature database updates. The ongoing evolution of attack tools makes it difficult to detect them using standard means;
- *resource limitations.* A shortage of financial resources complicates the acquisition of modern equipment and software for cybersecurity. There is also a shortage of qualified specialists due to low salaries or other restrictions.
- *imperfect regulatory framework*. The lack of clear guidelines for responding to cyberattacks can lead to chaos in the incident management process.
- *difficulty in identifying the source of the threat.* Attackers often hide their activities using VPNs, anonymous networks (Tor), or proxy servers. Multi-stage attacks, which involve various intermediate steps, complicate analysis. There is a lack of hardware or software to identify the source of attacks.
- *communication issues between departments.* IT departments and security services often work in isolation, slowing information exchange. There is a lack of unified protocols and standardized processes for incident response. There is also poor coordination between government structures and the private sector during joint responses to threats.

The outlined challenges highlight the need for a comprehensive approach to cybersecurity, including technological solutions, staff training, and improving the regulatory framework. The Cybersecurity Strategy of Ukraine [16], approved by the Decree of the President of Ukraine on 26.08.21, No. 447/2021, defined new challenges and cyber threats and emphasized the role of ensuring cybersecurity as one of the priorities in Ukraine's national security system.

Ukraine is actively developing and improving its legislative framework to counter cyber threats, especially in hybrid warfare and the growing scale of cyberattacks. The key documents shaping cybersecurity's regulatory and legal framework include the Constitution of Ukraine, which provides the basis for protecting information and citizens' rights in the digital space. The Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" [17], dated 05.10.2017, No. 2163-VIII, defines the legal and organizational foundations for protecting the vital interests of individuals and citizens, society, and the state, as well as the national interests of Ukraine in cyberspace. It outlines the main goals, directions, and principles of state policy in the field of cybersecurity in Ukraine, the powers and responsibilities of state bodies, enterprises, institutions, organizations, individuals, and citizens in this area, and the basic principles for coordinating their activities to ensure Ukraine's cybersecurity.

The Criminal Code of Ukraine dated 05.04.2001, No. 2341-III [18], provides for criminal liability for crimes in the field of cybersecurity, in particular for:

- unauthorized interference with the operation of electronic computing machines (computers), automated systems, computer networks, or telecommunication networks (Article 361);
- development with the purpose of using, distributing, or selling malicious software or technical tools, as well as their spread or sale (Article 361-1);
- unauthorized sale or distribution of restricted-access information stored in electronic computing machines (computers), automated systems, computer networks, or media containing such information (Article 361-2).

The Law of Ukraine "On Information," dated 13.01.2011, No. 2938-VI [19], regulates the fundamentals of information security, data protection, and legal relations in information processing. The Law of Ukraine, "On Information Protection in Information and Telecommunication Systems," dated 05.07.1994, No. 80/94-VR [20], establishes requirements for the

technical protection of information in information systems and obliges critical infrastructure operators to implement cybersecurity systems.

The National Security and Defense Council of Ukraine's decision, "On the Cybersecurity Strategy of Ukraine" [21], dated May 14, 2021, aims to strengthen the cybersecurity resilience of critical infrastructure and ensure the protection of state and private information systems. The Law of Ukraine "On the State Service of Special Communications and Information Protection of Ukraine," dated February 23, 2006 [22], establishes the legal foundations for the organization and activities of the State Service of Special Communications and Information Protection of Ukraine, following the Constitution of Ukraine. The Law of Ukraine, "On Electronic Trust Services," dated October 5, 2017 [23], regulates electronic signatures and ensures the security of digital transactions.

International agreements play a unique role in the fight against cybercrime. In particular:

1. The Budapest Convention [24] was ratified by Ukraine in 2005, with some essential reservations, including the criminalization in national legislation of the development or use of software or hardware for unauthorized access to, data interception, or interference with data or systems.

2. The Decree of the President of Ukraine dated February 1, 2022, No. 37/2022 "On the Decision of the National Security and Defense Council of Ukraine dated December 30, 2021, 'On the Implementation Plan of the Cybersecurity Strategy of Ukraine'" [25].

3. The Action Plan for the Implementation of the Provisions of the Cybersecurity Strategy of Ukraine for 2023–2024, approved by the Resolution of the Cabinet of Ministers of Ukraine on December 19, 2023, provides for "the creation of cyber troops within the Ministry of Defense, ensuring their adequate financial, personnel, and technical resources to deter armed aggression in cyberspace and to repel the aggressor" [26].

4. The Resolution of the Cabinet of Ministers of Ukraine dated April 4, 2023, No. 299, "Some Issues of Cybersecurity Entities' Response to Various Types of Events in Cyberspace" [27] and others.

Since the laws regulating cybersecurity were adopted at different times, their terminology is often inconsistent, and the division of powers between cybersecurity agencies remains unclear. As a result, Ukraine's cybersecurity legal framework requires a comprehensive review. In addition, the legislation contains some gaps and ambiguities, among which the following aspects are particularly important:

- inconsistency of national legislation with international obligations;
- inconsistency in terminology;
- lack of regulation of critical infrastructure;
- absence of provisions for conducting information security audits of critical infrastructure (CI);
- duplication of accountability;
- lack of clear requirements for CI asset managers and digital service providers to report cyber incidents;
- absence of a strategic cybersecurity plan; and tough budget constraints that restrict the government's ability to offer competitive salaries to attract and retain the required cybersecurity professionals.

A significant shortcoming of the legislative framework for combating cybercrime is the lack of clear regulation in the Criminal Code of Ukraine regarding electronic evidence, which must be submitted exclusively as electronic documents. Files or other digital traces are typically not signed with electronic signatures, as it is difficult to imagine a hacker deliberately performing such actions. Introducing the possibility of using electronic evidence in criminal cases would facilitate more effective cooperation between parties that have signed relevant international agreements in the investigation of crimes and proceedings related to the use of computer systems and data. Furthermore, to effectively implement the necessary provisions of the Budapest Convention, the Ukrainian government must take steps to provide more comprehensive and detailed definitions of cybersecurity concepts, such as 'service user' and 'service user information.

Ukraine's partner countries are actively analyzing the experiences and lessons of the russia-Ukraine cyber war. In their reports, they emphasize that Western assistance has played a key role in strengthening Ukraine's cyber resilience, significantly enhancing its ability to counter cyberattacks. At the same time, Ukraine has demonstrated an effective strategy for ensuring the resilience of critical functions. This strategy is based on the understanding that even the most advanced security measures can be bypassed; therefore, it is essential to ensure the continuity of core services through alternative means.

Some researchers note that Ukraine is currently better adapted to cyber confrontation and responding to new challenges in cyberspace than even the United States and its private sector, particularly industrial enterprises. A key priority remains the further development of information protection systems for critical infrastructure, based on best international practices. This includes the adoption of a special law on critical infrastructure protection, which would provide comprehensive regulation of the main directions, mechanisms, and legal frameworks for safeguarding critical infrastructure. Cyberattacks, which have become an integral part of modern conflicts, are used to destroy critical infrastructure, destabilize the economy, manipulate the information space, and undermine trust in state institutions. The increasing number and complexity of attacks, as seen in Ukraine’s case, highlight the importance of adapting to new challenges in cyberspace.

6. Conclusions

It is proved that enhancing Ukraine's cyber resilience requires the implementation of the following priority tasks: the introduction of advanced cyber threat monitoring systems (e.g., AI-based solutions), the establishment of cyber forces capable of countering threats at the national level, the implementation of continuous training programs for cybersecurity specialists, raising awareness among employees of public and private organizations about basic cyber threats such as phishing and social

engineering, the use of modern encryption tools to protect data, the deployment of integrated cybersecurity systems for network monitoring and rapid threat response, improving preparedness for supply chain attacks, and enhancing the security of critical infrastructure through regular audits and penetration testing.

It is established that strengthening coordination with international organizations is crucial for effectively counteraction to cyber threats that accompany the development of the digital economy and information society. The development of a comprehensive cybersecurity system focused on the prevention and deterrence of cyber threats will be a significant step toward enhancing cyber resilience. This will enable Ukraine not only to adapt to dynamic changes in cyberspace but also to stay ahead of them, ensuring a rapid response to new challenges.

References:

1. «Uriadova komanda CERT-UA v 2023 rotsi opratsiuvala 2543 kiberintsydenty», *Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy*, [Online], available at: https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti
2. Hrytsyshen, D.O., Yevdokymov, V.V., Savchuk, S.O. and Korzun S.V. (2024), *Stratehiia intehratsii derzhavnoi polityky protydii kiberzlochynnosti v yevropeisku systemu kiberbezpeky*, monohrafiia, Vydavnychyi dim «Buk-Druk», Zhytomyr, 312 p.
3. Didenko, A.S. (2019), «Derzhavna polityka u sferi protydiï kiberzlochynnosti yak obiekt administratyvno-pravovoho rehuliuvannia», *Materialy konferentsii «Kharkivskyy natsionalnyy universytet vnutrishnikh sprav: 25 rokiv dosvidu ta pohliad u maybutnie (1994–2019 rr.)»*, Kharkiv, 154 p., [Online], available at: https://univd.edu.ua/general/publishing/konf/22_11_2019/pdf/73.pdf
4. Didenko, A.S. (2020), «Meta, zavdannia ta pryntsypy derzhavnoi polityky u sferi protydii kiberzlochynnosti», *Pravo i bezpeka*, No. 1 (76), pp. 53–59.
5. Diorditsa, I.V. (2017), «Poniattia ta zmist kiberzlochynnosti», *Hlobalna orhanizatsiia soiuznytskoho liderstva*, [Online], available at: http://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti
6. Diorditsa, I.V. (2016), «Poniattia ta zmist natsionalnoï systemy kiberbezpeky», *Hlobalna orhanizatsiia soiuznytskoho liderstva*, [Online], available at: http://goal-int.org/ponyattya-ta-zmist-nacionalnoi
7. Kotsman, I. (2024), «Derzhavne rehuliuvannia protydiï kiberzlochynnosti v ukraïni: poniattia ta osnovni napriamky», *Publichne upravlinnia ta administruvannia v Ukraini*, No. 40, pp. 245–252.
8. Orlov, O.V. and Onyshchenko, Yu.M. (2013), «Teoriia ta praktyka derzhavnoho upravlinnia», *Aktualni napriamy derzhavnoi polityky Ukrainy u sferi borotby z kiberzlochynnistiu*, No. 1 (44), pp. 3–9.
9. Orlov, O.V. and Onyshchenko, Yu.M. (2014), «Derzhavna polityka pidhotovky kadriv z poperedzhennia kiberzlochynnosti v Ukraini», *Aktualni problemy derzhavnoho upravlinnia*, pp. 230–236, [Online], available at: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=njuu_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21COLORTERMS=0&S21P03=I=&S21STR=%D0%9669634:%D0%A5.%D1%84./2014/1
10. Yang, E. (2003), *Yak napysaty diievyyi analitychnyyi dokument u haluzi derzhavnoi polityky*, Praktychnyyi posibnyk dlia radnykiv z derzhavnoï polityky u Tsentralnoi i Skhidnoi Yevropy, Translated by eng. Sokolyk, S., K.I.S., Kyïv, 120 p.
11. Verkhovna Rada Ukrainy (2021), *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku «Pro Stratehiiu kiberbezpeky Ukrainy»*, Ukaz Prezydenta Ukrainy № 447/2021 vid 26.08.2021 r., [Online], available at: https://zakon.rada.gov.ua/laws/show/447/2021#Text
12. *Microsoft*, «Defending Ukraine: Early Lessons from the Cyber War», [Online], available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK
13. *SWP*, «Microsoft Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine», [Online], available at: https://www.swp-berlin.org/en/swp/about-us/organization/swp-projects/european-repository-on-cyber-incidents-eurepoc
14. *Grant Writing USA*, «Home – Grant Writing USA», [Online], available at: https://www.grantwritingusa.com
15. *Statista*, «Cyber incidents targeting governments global by attack vector 2023», [Online], available at: https://www.statista.com/statistics/1428581/government-worldwide-targeted-cyber-incidents-by-attack-vector/
16. Rada Natsionalnoi Bezpeky i Oborony Ukrainy (2021), *Pro Stratehiiu kiberbezpeky Ukrainy*, Rishennia vid 14.05.2021 r. [Online], available at: https://zakon.rada.gov.ua/laws/show/n0055525-21#Text
17. Verkhovna Rada Ukrainy (2017), *Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy*, Zakon Ukrainy vid 05.10.2017 r. No. 2163-VIII, [Online], available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text
18. Verkhovna Rada Ukrainy (2001), *Kryminalnyi Kodeks Ukrainy*, document No. 2341-III vid 05.04.2001 r., [Online], available at: https://zakon.rada.gov.ua/laws/show/2341-14#Text
19. Verkhovna Rada Ukrainy (2011), *Pro vnesennia zmin do Zakonu Ukrainy «Pro informatsiiu»*, Zakon Ukrainy vid 13.01.2011 r. No. 2938-VI, [Online], available at: https://zakon.rada.gov.ua/laws/show/2938-17#Text
20. Verkhovna Rada Ukrainy (1994), *Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh*, Zakon Ukrainy vid 05.07.1994 r. No. 80/94-VR, [Online], available at: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text
21. Verkhovna Rada Ukrainy (2021), *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku «Pro Stratehiiu kiberbezpeky Ukrainy»*, Ukaz Prezydenta Ukrainy vid 26.08.2021 r. No. 447/2021, [Online], available at: https://zakon.rada.gov.ua/laws/show/447/2021#Text
22. Verkhovna Rada Ukrainy (2006), *Pro Derzhavnu sluzhbu spetsialnoho zviazku ta zakhystu informatsii Ukrainy*, Zakon Ukrainy vid 23.02.2006 r. No. 3475-IV, [Online], available at: https://zakon.rada.gov.ua/laws/show/3475-15#Text
23. Verkhovna Rada Ukrainy (2017), *Pro elektronni dovirchi posluhy*, Zakon Ukrainy vid 05.10.2017 r. No. 2155-VIII, [Online], available at: https://zakon.rada.gov.ua/laws/show/2155-19#Text
24. Rada Yevropy (2005), *Konventsiia pro kiberzlochynnist*, document vid 23.11.2001 r., [Online], available at: https://zakon.rada.gov.ua/laws/show/994_575#Text
25. Verkhovna Rada Ukrainy (2021), *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku «Pro Stratehiiu kiberbezpeky Ukrainy»*, Ukaz Prezydenta Ukrainy vid 26.08.2021 r. No. 447/2021, [Online], available at: https://zakon.rada.gov.ua/laws/show/447/2021#Text
26. Kabinet Ministriv Ukrainy (2023), *Pro zatverdzhennia planu zakhodiv na 2023-2024 roky z realizatsii Stratehii kiberbezpeky Ukrainy*, Rozporiadzhennia vid 19.12.2023 r. No. 1163-r, [Online], available at: https://zakon.rada.gov.ua/laws/show/1163-2023-р#Text
27. Kabinet Ministriv Ukrainy (2023), *Deiaki pytannia reahuvannia subiektamy zabezpechennia kiberbezpeky na rizni vydy podii u kiberprostori*, Postanova vid 04.04.2023 r. No. 299, [Online], available at: https://zakon.rada.gov.ua/laws/show/299-2023-п#Text