Economic Affairs, Vol. **69**(Special Issue), pp. 61-69, February 2024
DOI: 10.46852/0424-2513.1.2024.8

AESSRA

Review Paper

Cybercrime and Information Protection in the Field of State Security: Current Threats and Measures for their Prevention

Viktor Ievdokymov[1*], Andrii Frikel[2], Volodymyr Polishchuk[3], Serhii Savchuk[4] and Inna Klimova[5]

[1]Rector of Zhytomyr Polytechnic State University, Zhytomyr, Ukraine
[2]Department of National Security, Public Management and Administration, Faculty of National Security, Law and International Relations, Zhytomyr Polytechnic State University, Zhytomyr, Ukraine
[3]Interregional Academy of Personnel Management, Kyiv, Ukraine
[4]Department of Management and Entrepreneurship, Zhytomyr Polytechnic State University, Zhytomyr, Ukraine
[5]Department of Economics, Management, Marketing and Hotel-Restaurant Business, Faculty of Socio-psychological, Zhytomyr Ivan Franko State University, Zhytomyr, Ukraine

*Corresponding author: rector@ztu.edu.ua (**ORCID ID:** 0000-0002-3577-081X)

Received: 21-10-2023 **Revised:** 20-01-2024 **Accepted:** 03-02-2024

ABSTRACT

The present research is a comprehensive analysis of the current state of cybercrime and its impact on national security. The focus is on identifying key threats in the digital space and developing strategies to prevent and counteract them in order to ensure state security. The research objectives include the analysis of the dynamics and evolution of cybercrime, the assessment of its impact on various aspects of national security, including information, economic and military spheres, and the development of strategies and methods for public and private entities to counter cyber threats. The methods of analyzing network interactions and the information approach with an emphasis on existing information actors were used in the research. The research has shown that cybercrime is constantly evolving, which is related to the emergence of new IT technologies and an increase in the number of users involved in information processes. The major categories of crimes are identified: illegal downloading or use of software, fraud and attacks exploiting vulnerabilities of systems. The necessity of joint efforts of various subjects in cybersecurity is also noted with a special emphasis on the role of the state. The academic paper emphasizes that cybersecurity in public governance is achieved through the unification of data exchange methods, using transport protocols such as HTTP. The study of information confrontation requires a detailed analysis of the main areas of cyber defense, including strategies for countering public governance systems, information and intelligence activities, electronic warfare, psychological confrontation, hacker operations, cyber and network warfare, economic information warfare and international information terrorism. The academic paper emphasizes that international information terrorism in the era of information confrontation is gaining new importance, in particular, due to the use of the information structure by terrorists to form network methods and influence information infrastructure facilities.

HIGHLIGHTS

- The escalating complexity and sophistication of cybercrimes, coupled with the growing number of Internet users and mobile devices, underscore the urgent need for comprehensive, state-led cybersecurity measures that go beyond traditional approaches to address evolving threats in a rapidly changing technological landscape.
- The multifaceted nature of cyber threats, ranging from information warfare and cyber espionage to hacker warfare and economic cyber-information warfare, highlights the importance of a holistic cybersecurity strategy that integrates public-

How to cite this article: Ievdokymov, V., Frikel, A., Polishchuk, V., Savchuk, S. and Klimova, I. (2024). Cybercrime and Information Protection in the Field of State security: Current Threats and Measures for their Prevention. *Econ. Aff.*, **69**(Special Issue): 61-69.

Source of Support: None; **Conflict of Interest:** None

private collaboration, standardized programming languages, and advanced technologies like two-factor authentication to safeguard national security in the face of evolving challenges in the global information space.

Keywords: Cybercrime, cybersecurity, information technology, state security tools, public governance system

The current reality shows that the world has observed a significant increase in the number of cybercrimes in recent decades. Both the motives and goals of the attackers are changing, and the level of threat from their actions continues to grow for states and state institutions. The aggravation of this issue requires an immediate and effective solution, given that cybercrime is becoming more complex and sophisticated and the effectiveness of investigations and counteraction in cyberspace is declining. The topic of cybersecurity is particularly relevant at the moment in light of the expenses for preventing and solving cybercrime in the context of state security. Legal entities and individuals seek to protect themselves in advance; however, criminals in cyberspace are constantly improving their methods, making this area important for constant monitoring and development of new solutions. The expansion of the capabilities of information technologies, especially the Internet, has led to increased interest on the part of individuals and organized criminal groups that use these technologies for illegal purposes. The availability of technologies, their low cost, and the possibility of obtaining significant profits with minimal risks and high anonymity make the fight against cybercrime one of the world's most pressing challenges (Eichensehr, 2022). The ongoing development of information technologies and the emergence of new ways to use them for criminal purposes threaten the security of global information networks and states in general. These are the reasons for the high relevance of our research.

LITERATURE REVIEW

In the course of our research, we will examine the concept of "crime in the field of computer information", referring to both scholarly and legislative definitions to gain a better understanding of this escalating phenomenon. The terms "cybercrime" and "crime in the field of computer information" are often used synonymously, although there are certain differences between them. For instance, Di Nicola, (2022) in his study defines crimes in the field of computer information without making a clear distinction between this term and the concept of "computer crimes".

The scientific works (Vakulyk *et al.* 2020; Wang, Su, Wang 2021) highlight the idea that the term "computer crime" was introduced to describe both completely new types of crimes targeting computers, networks and their users, as well as traditional crimes committed with the use of computer hardware.

Shablystyi *et al.* (2019) defined "computer crimes" as a category that has a clear definition and includes both crimes in the field of computer information and crimes committed in the field of information and communication technologies, proposing to define them as information crimes; crimes in which computers and networks are tools for committing illegal actions.

In particular, (Collier *et al.* 2021; Jordan & Weller, 2018) interpret cybercrime as a concept that encompasses all illegal actions that are performed or carried out using information and communication technologies.

The term "cybercrime" means actions aimed at violating the confidentiality, compromising the integrity or restricting access to computer data or systems, which is the core of the concept of cybercrime (Avanesova *et al.* 2021). In a broader sense, this includes crimes committed using computers for personal or financial gain or harm, including the use of personal data and information stored in computer systems (Holt *et al.* 2022).

Several scholarly works, such as Akoto, 2022; Dupont, Whelan, 2021, note that "cybercrime" covers crimes related to both the use of computer technologies and global networks. At the same time, "computer crime" more specifically refers to crimes against computer systems or data.

Such scholars as (Chowdhury *et al.* 2022; Leukfeldt, Lavorgna, Kleemans, 2017; Tropina, 2020) show that crimes committed in global computer networks usually have the following features: (a) high secrecy during the commission of crimes; (b) cross-border nature, where the criminal, the target of the crime and the victim may be located in different countries; (c) special qualifications of criminals and the intellectual nature of their actions; (d) the possibility of automated crimes in several places at the same time; e() the difficulty of preventing and suppressing such crimes by traditional methods. In general, we can state that nowadays cybercrime includes a wide range of illegal actions, from unauthorized access to state computer networks and identity theft to financial espionage and money laundering.

AIMS

The main purpose of the research is to provide a thorough analysis of the current state of cybercrime and its impact on state security. The research aims to identify the key threats arising in the digital space and develop effective strategies and methods to prevent and counteract these threats in the context of ensuring state security.

The Research Objectives: (1) to study the dynamics of cybercrime, with an emphasis on the latest methods and tactics used by criminals; (2) to assess how cybercrime affects various aspects of national security, including information, economic and military spheres; (3) to suggest strategies and methods that can be used by government agencies and the private sector to prevent and minimize risks caused by cyber threats; (4) to provide practical recommendations for strengthening state cybersecurity at various levels – from the individual user to national government agencies.

MATERIALS AND METHODS

In the framework of our research, the following scientific, methodological and analytical approaches were applied:

1. An approach to analyzing network interactions. This method consists of studying and investigating the interrelations and interactions between various elements within a particular network. It includes identifying and exploring the nodes (or participants) of the network and the connections between them. These nodes can be individuals, groups, organizations, or system components, and the links can be physical, social, or economic. The method covers the analysis of the distribution of information, resources, and influence in the network, and examines how these processes affect the behavior of participants and the network as a whole. This approach is used particularly in the context of state information networks to analyze the processes of influence, information dissemination and the formation of public opinion. The method helps identify key nodes and connections that are critical to the functioning and sustainability of the information network.

2. Information approach with a focus on existing information subjects. Information influence becomes the main tool for managing society, replacing physical action, which for centuries was considered the only means of impact. In the era of informatization, information influence is gaining special significance, which makes cybersecurity one of the key aspects of public governance and state security. Activities in the field of state cybersecurity are aimed at protecting the rights and freedoms of citizens, society and the state. In the context of public governance, cybersecurity is defined as a state in which an individual, society and the country are protected from internal and external information threats. This condition guarantees the observance of constitutional human and civil rights and freedoms, ensures a decent standard of living for citizens, supports the sovereignty, territorial integrity and sustainable social-economic development of the state.

3. The dualistic approach to the definition of “cybercrime” has also been recognized at the state level of governance. It is divided into two categories: (1) computer crimes in the narrow sense, which are illegal acts created to breach the protection of computer systems and the data they process; (2) computer crimes in a broad sense, covering illegal actions related to the use of computer systems or networks, including illegal storage, distribution or offering of information through computer systems or networks. Thus, the dualistic approach to the definition of “computer crime” is considered to be the most reasonable since it makes it possible to comprehensively assess the complexity, diversity and multilevel nature of the phenomenon under consideration, as well as to find a balance between different scientific concepts.

RESULTS

Cybercrime in the field of state security is constantly evolving due to the improvement of IT technologies and the emergence of new ones, as well as the increase in the number of users involved in information processes. This includes the expansion of cyberspace due to the growing number of Internet users and mobile devices, as well as the transition to electronic document management in government organizations and institutions. The study conducted by McAfee among 100 IT departments from 15 countries responsible for the security of critical resources found that in 2022, 82% of them experienced cyberattacks (Chief Economists Outlook, 2023). Currently, Ukraine, along with the United States and China, is one of the leading countries in terms of the number of cyberattacks. Crimes in this area can be classified into three main categories: (1) illegal downloading or use of software; (2) fraud and deception; (3) attacks that exploit system vulnerabilities and unauthorized access to digital data and/or networks of government agencies and institutions (Lavorgna, 2023). The volume of such crimes has increased significantly over the past two years because of the growing number of websites and networks that provide access to information (Fig. 1).

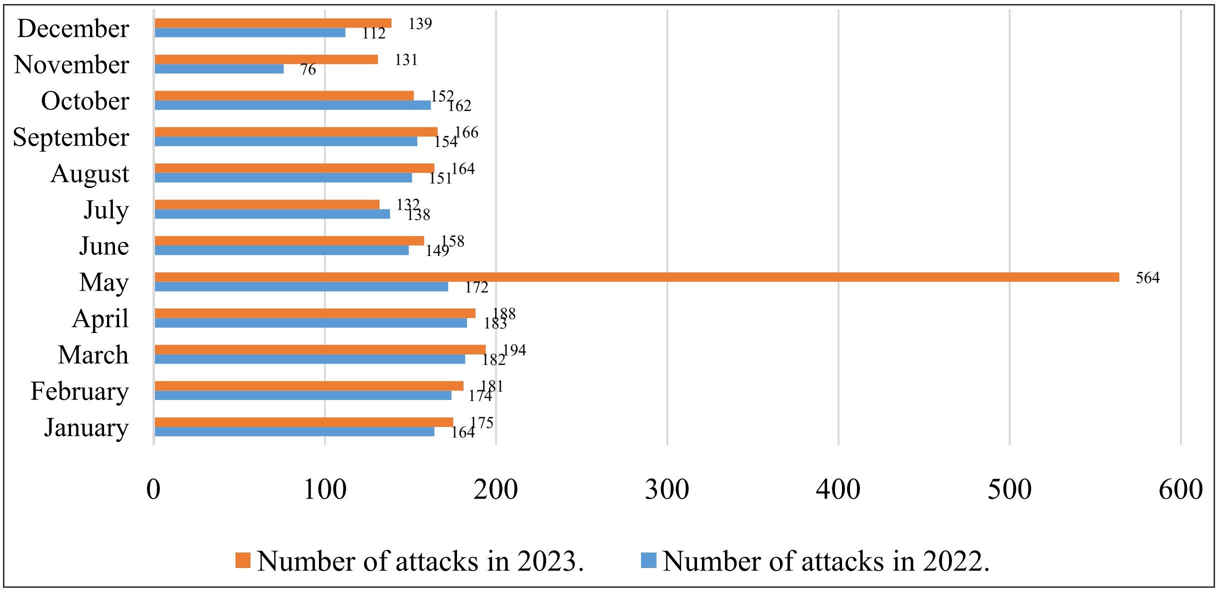
Cyber technologies and fraudulent schemes exploit vulnerabilities in state security systems, using social engineering techniques and lack of awareness of end users about the necessary security measures to protect against online threats. Malicious unauthorized access is performed when a criminal uses various methods, such as viruses or worms, to control someone else's system without the owner's permission (Anttila, 2022). Table 1 demonstrates the targets and different types of threats, and the illegal actions can be conducted in the forms of attacks discussed above.

There is no doubt that the unique features of information systems, especially the Internet, "necessitate joint efforts of various subjects, both public and private", in addressing state cybersecurity issues. Nevertheless, the key role in this process should be played by the state, which has unique capabilities to effectively counter cybercrime and create conditions for protecting the most vulnerable entities, allowing them to develop more reliable state cybersecurity systems (Dumchykov & Utkina & Bondarenko, 2022). Depending on the goals, objectives and resources of cyberspace actors, three main levels of threats to state information security and their corresponding types of threats can be distinguished, as shown in Fig. 2.

This approach also recognizes the special danger to the state system of governance posed by such destructive actions of states in cyberspace as information warfare and cyber espionage. In turn, the misuse of information and communication technologies (ICT) for criminal and terrorist purposes poses a serious threat to both the public and private sectors. Hacking is a significant local threat that affects individual users and local networks. In this regard, the risk of destructive actions by insiders remains relevant at all levels. The model of cybersecurity management of state institutions is shown in Fig. 3.

Integration of information protection processes in the field of state security involves the application of consistent procedures, in which special applications are used at certain stages. Information is processed at these stages with the help of applications, and the process functions are performed through a specialized subsystem. This method of integration is based on the "WorkFlow" technology (Kormych, Zavhorodnia 2023). It is proposed to use the model of two-factor authentication of civil servants in the development of the state cybersecurity system (Fig. 4).

The proposed model is based on two types of two-factor authentication: an in-app authenticator and login verification through mobile applications. The presented model and algorithm for protecting information in the monitoring system are based on a combination of two factors: a static and a temporary password. A static password (the first factor) is set by the user and used to create an account. One-time passwords that act as an additional factor are generated on the server according to the described algorithm and are active for a limited time, which is twenty seconds for each authentication session. Reused passwords are not allowed, which is an obstacle for an attacker trying to intercept them. It should be noted that the password length is 6 characters and it is changed every 10 seconds. Given this, cracking such a password within the allotted



Source: *(Cyber Threats Forecast 2024).*

Fig. 1: The number of attacks with significant data breaches in 2022 and 2023 on a global scale

Table 1: Objects and types of cyber threats

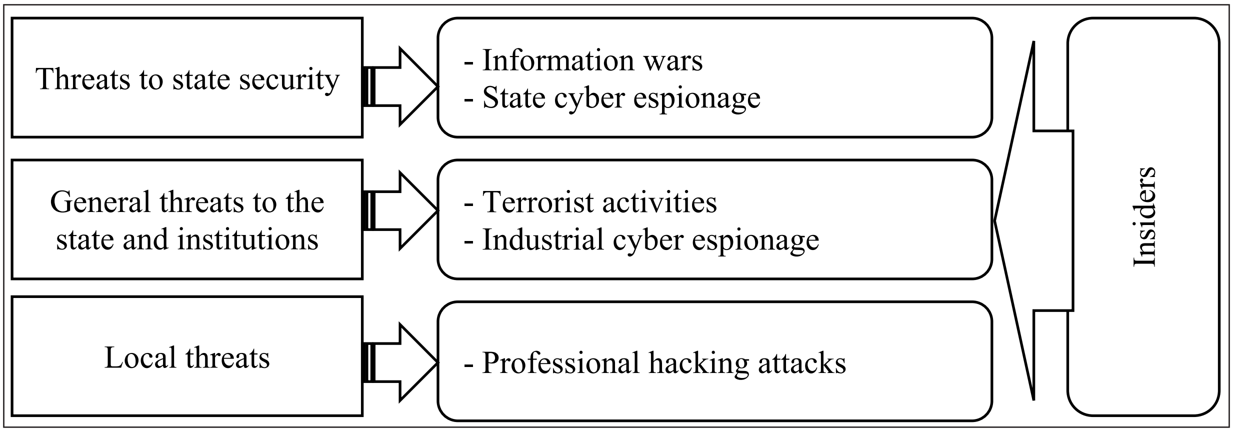
The object of threats	Types of threats
Civil society	Manipulation of identity through the collection of personal data and attacks on the computers of civil servants. Removal and disclosure of confidential information or data intended for a limited number of users. Financial frauds. Dissemination of malicious content.
Business environment	Negative impact on the Internet security systems of government authorities. Disruption of the operation of the information infrastructure. Paralyzing online document management systems and geographic information systems. Hacker attacks on government websites.
State system	Attacks on important government management systems (e-government, official websites of government agencies). Economic restrictions (large-scale suspension of payment systems, treasuries, and the national bank). Physical attacks on personal computers and critical infrastructure of state-owned enterprises and institutions.

Source: *Compiled by the authors on the basis of (Cybersecurity in the United Nations system organizations, 2021; Makedon, et al. 2019).*

time is a significant challenge since more than 1 million combinations need to be searched (UNDP GUIDE A Study of Regional Frameworks, 2023).

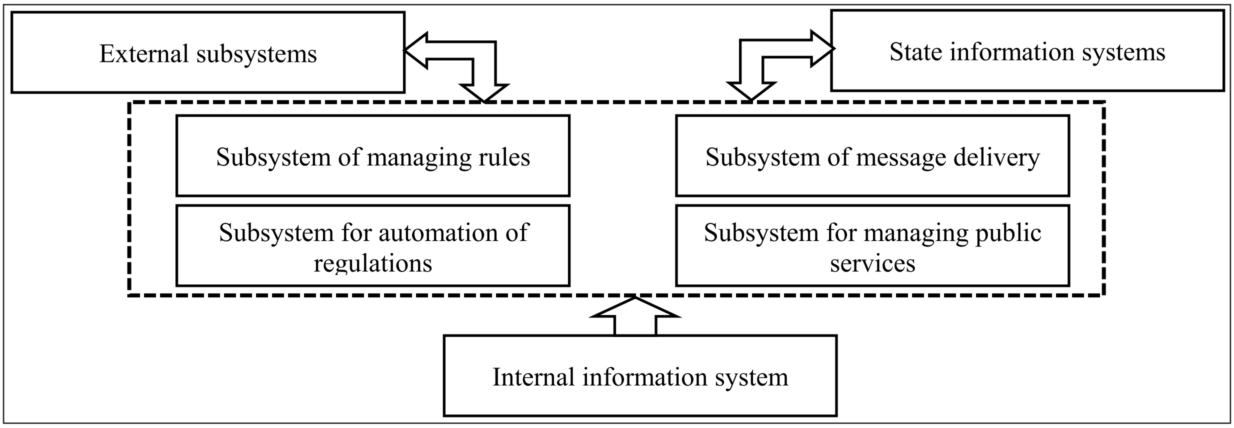
Programs operating at the middle level integrate key program components. Leading companies are actively developing integrated solutions for corporate information systems. These solutions include, for example, Oracle 10g, Microsoft BizTalk Server, IBM WebSphere, and SAP Netweaver. Microsoft BizTalk Server, which implements the processing and transfer functions in the electronic document management system, is an example.

The language format plays a key role in ensuring state cybersecurity of processes in the technological aspect. Programming languages used in integrated information systems are standardized. These standards include Express with STEP, the XML markup language, and the EDIFACT data exchange format. The RDFS metadata language and the


Threats to state security
General threats to the state and institutions
Local threats
- Information wars
- State cyber espionage
- Terrorist activities
- Industrial cyber espionage
- Professional hacking attacks
Insiders

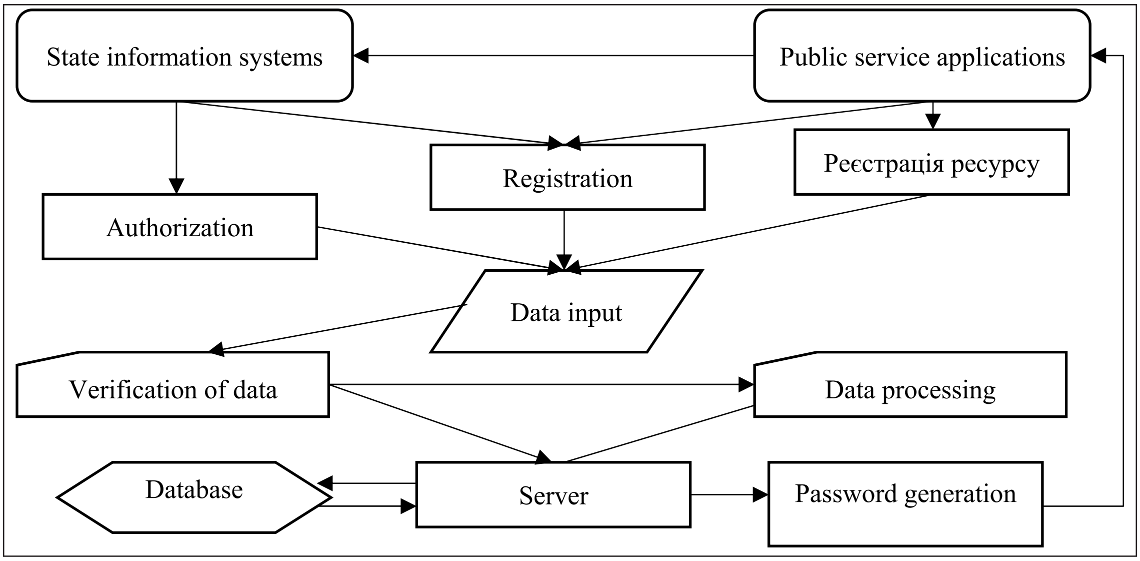
Source: *Developed on the basis of (Chief Economists Outlook, 2023).*

Fig. 2: Levels of threats to state information security


External subsystems
State information systems
Subsystem of managing rules
Subsystem of message delivery
Subsystem for automation of regulations
Subsystem for managing public services
Internal information system

Source: *developed by the authors.*

Fig. 3: Cybersecurity management at the level of government authorities



Source: *Developed by the authors.*

Fig. 4: Model of the proposed two-factor authentication of civil servants

OWL ontology representation language are used to maintain consistency in databases (Heidi, 2022).

In summary, it can be stated that cybersecurity in state governance is achieved through the unification of data exchange methods, for which transport protocols are used. The HTTP protocol is widely used on the Internet to organize interactions between the client and the server. WSDL, SOAP, and UDDI protocols are applied to search for the required server and establish communication in the network environment. In this context, the HTTP protocol is the vehicle for SOAP messages (McAfee & Brynjolfsson, 2017).

Studying the issues of information confrontation, including identifying opportunities for planning actions to influence or counteract information influences, requires a detailed analysis of the main areas of cyber defense. In addition to purely civilian cyber defense, a modern state must be able to actively counter cyber threats by developing active countermeasures. These events are of great relevance and importance for modern Ukraine (Reuters, 2022). Our research has identified the following key directions:

1. Strategy of cyber information counteraction to management systems. This strategy is perceived as a military tactic aimed at eliminating control systems and isolating the enemy's management structures in order to disrupt its military leadership. Such a confrontation can be achieved through direct destruction of control nodes or through disruption of telecommunication networks coordinating the management. The method of counteraction is chosen in accordance with certain tactical and strategic objectives. The significance of cyber information operations against management systems lies in their potential effectiveness in the initial stages of a conflict, creating the basis for a bloodless victory over the enemy. However, such advantages can be reduced by the enemy due to the decentralization of monitoring systems and the so-called "network warfare" (Johansson & Johansson, (2022). These operations can be viewed as an evolution of traditional operational intelligence, although they have significant differences based on the fact that the information collected is directly transmitted to the operation's participants. When military intelligence information is delivered to command centers, it is analyzed and transformed into orders for execution there. This involves adapting operational intelligence to decentralized systems of military command and control and combat operations, which requires significant changes in the collection, processing and distribution of intelligence information.

2. Electronic confrontation. It differs from the first direction, which implies fighting with or through information systems. The purpose of electronic confrontation is to reduce the enemy's information capabilities. This includes combating enemy communications networks, electronic warfare and cryptographic warfare.

3. Psychological cyber confrontation. Here, the impact on the human mind and psyche is directly highlighted rather than information systems. Psychological struggle includes manipulation of public consciousness and views of different social groups. In NATO countries, the following main types of actions are distinguished within psychological warfare: the demoralization of military personnel, operations against the military command, and even actions designed to govern (Taherdoost, 2022).

4. Hacker warfare means the use of computer technologies to illegally access or disrupt the operation of enemy systems. The hacker fight is mostly focused on computer network components and information resources. Hacking processes are characterized by their software nature, as opposed to hardware attacks. Many Western experts argue that the current information confrontation is mostly driven by hacker warfare. The most common tools in hacker warfare are computer worms, viruses, Trojans, malware for a permanent device, and logic bombs, which can be considered as examples of information weapons.

5. Cyber and network warfare, which, despite their technical names, are not much related to information technologies and cover a wide range of information warfare issues, including organizational, tactical, doctrinal, technical and strategic aspects. Cyber warfare plays an important role in the modern protection of state cyberspace, especially in high-intensity conflicts and with the application of the latest technologies (Ross & Maynard, 2021).

6. Economic cyber-information warfare, where the main format is information blockade. In the

context of globalization and the digital economy, an information blockade can provide a hidden influence on the enemy. This differs from traditional economic sanctions since it can be disguised as random hacker attacks or failures in information systems, although it does not exclude the possibility of overt state influence (Makedon, et al. 2022).

We emphasize the need to strengthen state cybersecurity at all levels, from the individual user to national government bodies and offer specific recommendations for protecting against cyber threats.

DISCUSSION

A significant change has recently been observed in the complex of factors that determine computer crime at the state level. In addition to the traditional social, economic, legal, personnel, organizational and technical aspects, political factors are becoming increasingly important. These include geopolitical aspects, including military-political, global economic and international political elements, as well as political and surveillance factors related to insufficient social and state control over cyberspace. Other important factors include political-criminal (including cyberterrorism, cyberextremism and hacktivism), political-information (cyberespionage) and political-institutional (misuse of IT technologies). The key point in the evolution of cybercrime, which turns it into a technotronic crime, is its self-determination. This process means the ability of computer crime to regenerate autonomously, that is, to reproduce crimes in the social environment on its own. These manifestations determine the prospects for further studies on modern cyber threats and measures to prevent them.

CONCLUSION

It is determined that computer crime is constantly evolving due to the improvement and emergence of new IT technologies, an increase in the number of Internet users and mobile devices, as well as the transition to electronic document management in organizations. Computer crime can be divided into illegal use of software, fraud, and attacks that exploit system vulnerabilities.

In cybersecurity, public-private collaboration is essential, but the state still has a major role to play. There are three main levels of cyber threats, each of which has its own specific types of threats. Actions of states in cyberspace, such as information warfare and cyber espionage, pose a particular threat to national security.

The use of WorkFlow technology and the development of state cybersecurity systems, in particular, the two-factor authentication model, are proposed to be crucial for ensuring cybersecurity. Using standardized programming languages and formats, such as XML, EDIFACT, RDFS, OWL, is important to ensure data interoperability and security. International information terrorism is becoming an important factor in the global information space, especially given the use of high-tech methods. Several main directions have been identified, including electronic warfare, psychological warfare, hacker warfare, cyber and network warfare, which should be taken into account when developing cybersecurity strategies.

REFERENCES

Akoto, W. 2022. Accountability and cyber conflict: examining institutional constraints on the use of cyber proxies. *Conflict Management and Peace Science*, **39**(3): 311–332.

Anttila, J. 2022. *Information security challenge of modern society*, **14**: 65-70. https://doi.org/10.14529/ped220206

Avanesova, N., Tahajuddin, S., Hetman, O., Serhiienko, Y. and Makedon, V. 2021. Strategic management in the system model of the corporate enterprise organizational development. *Economics and Finance*, **1**(9): 18–30.

Chief Economists Outlook, 2023. https://www.weforum.org/reports/chief-economists-outlook-may-2023?gclid=CjwKCAjww7KmBhAyEiwA5-PUSiwfPlcu3cw8SC7qCW5qZVZEqL81p_tMqx52LvcEtSaFplgPQYGrrBoCn6AQAvD_BwE

Chowdhury, N., Nystad, E., Reegård, K. and Gkioulos, V. 2022. Cybersecurity training in Norwegian critical infrastructure companies. *International Journal of Safety and Security Engineering,* **12**(3): 299-310.

Collier, B., Clayton, R., Hutchings, A. and Thomas, D. 2021. Cybercrime is (often) boring: Infrastructure and alienation in a deviant subculture. *The British Journal of Criminology*, **61**(5): 1407–1423.

Cyber Threats Forecast, 2024. https://www.h-x.technology/blog/cyber-threats-forecast-2024

Cybersecurity in the United Nations system organizations. 2021. https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf

Di Nicola, A. 2022. Towards digital organized crime and digital sociology of organized crime. *Trends Organized Crime*. https://doi.org/10.1007/s12117-022-09457-y

Dumchykov, M. & Utkina, Maryna & Bondarenko, Olha. 2022. Cybercrime as a Threat to the National Security of the Baltic States and Ukraine: The Comparative Analysis. *International Journal of Safety and Security Engineering*, **12**: 481-490.

Dupont, B. and Whelan, C. 2021. Enhancing relationships between criminology and cybersecurity. *Journal of Criminal Law and Criminology*, **54**(1): 76–92.

Eichensehr, K. 2022. Ukraine, cyberattacks, and the lessons for international law. *AJIL Unbound*, **116**: 145–149.

Heidi, A. 2022. Digital transformation, development and productivity in developing countries: is artificial intelligence a curse or a blessing? *Review of Economics and Political Science*, **7**(4): 238–256.

Holt, T.J., Chermak, S.M., Freilich, J.D., Turner, N., Greene-Colozzi, E. 2022. Introducing and Exploring the Extremist Cybercrime Database (ECCD). *Crime & Delinquency*, 0011128722108389.

Johansson, E. and Johansson, K.M. 2022. Along the government–media frontier: Press secretaries offline/online. *Journal of Public Affairs*, **22**(Suppl. 1). https://doi.org/10.1002/pa.2759

Jordan, K. and Weller, M. 2018. Academics and social networking sites: benefits, problems and tensions in professional engagement with online networking. *Journal of Interactive Media in Education*, pp. 1-9. https://doi.org/10.5334/jime.44

Lavorgna, A. 2023. Unpacking the political-criminal nexus in state-cybercrimes: a macro-level typology. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-023-09486-1

Leukfeldt, E.R., Lavorgna, A. and Kleemans, E.R. 2017. Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *The European Journal on Criminal Policy and Research*, **23**(3): 287–300.

Liudmyla, Kormych, Yuliia and Zavhorodnia. 2023. The concept of modern political confrontation in cyber space. *Journal of Cybersecurity*, **9**(1).

Makedon, V., Zaikina, H., Slusareva, L., Shumkova, O. and Zhmaylova, O. 2019. Rebranding in the Enterprise Market Policy. *Proceedings of the 34rd International Business Information Management Association Conference*, IBIMA 2019: Vision 2025: Education Excellence and Management of Innovations through Sustainable Economic Competitive Advantage, 9472-9476

Makedon, V., Krasnikova, N., Krupskyi, O. and Stasiuk, Y. 2022. Arrangement of Digital Leadership Strategy by Corporate Structures: A Review. *Ikonomicheski Izsledvania*, **31**: 19-40.

McAfee, A. and Brynjolfsson, E. 2017. *Machine, Platform, Crowd: Harnessing Our Digital Future*. New York: W.W. Norton & Company.

Reuters, 2022. The cyber war between Ukraine and Russia: An overview. https://www.reuters.com/world/europe/factbox-the-cyber-war-between-ukraine-russia-2022-05-10/

Ross, P. and Maynard, K. 2021. Towards a 4th industrial revolution. *Intelligent Buildings International*, **13**(3): 159-161.

Shablystyi, V., Prymachenko, V., Filipp, A., Doroshenko, L., Burbyka, V. 2019. Legal principles of cyber protection of critical infrastructure facilities. *Journal of Legal, Ethical and Regulatory Issues*, **22**(6): 1-6.

Taherdoost, H. 2022. Cybersecurity vs. Information Security. *Procedia Computer Science*, **215**: 483-487.

Tropina, T. 2020. *Cybercrime: setting international standards*. Routledge handbook of international cybersecurity. Routledge, London, pp. 148–160.

UNDP GUIDE A Study of Regional Frameworks, 2023. https://www.undp.org/sites/g/files/zskgke326/files/2023-04/UNDP%20Drafting%20Data%20Protection%20Legislation%20March%202023.pdf

Vakulyk, O., Petrenko, P., Kuzmenko, I., Pochtovyi, M. and Orlovskyi, R. 2020. Cybersecurity as a component of the national security of the state. *Journal of Security and Sustainability Issues*, **9**: 775-784.

Wang, P., Su, M. and Wang, J. 2021. Organized crime in cyberspace: how traditional organized criminal groups exploit the online peer-to-peer lending market in China. *The British Journal of Criminology*, **61**(2): 303–324.