State Management Mechanisms for the Exchange of Information Regarding Cyberattacks, Cyber Incidents and Information Security Incidents

Myroslav Kryshtanovych †, Igor Britchenko ††, Peter Lošonczi †††, Tetiana Baranovska††††, Ulyana Lukashevska †††††

† Lviv Polytechnic National University, Lviv, Ukraine
†† Higher School of Insurance and Finance, Sofia, Bulgaria
††† University of Security Management in Košice, Slovakia
†††† Zhytomyr Polytechnic State University, Zhytomyr, Ukraine
††††† Lviv Polytechnic National University, Lviv, Ukraine

Abstract
The main purpose of the study is to determine the key aspects of the mechanisms of state management of the exchange of information about cyberattacks, cyber incidents, and information security incidents. The methodology includes a set of theoretical methods. Modern government, on the one hand, must take into account the emergence of such a new weapon as cyber, which can break various information systems, can be used in hybrid wars, influence political events, pose a threat to the national security of any state. As a result of the study, key elements of the mechanisms of state management of the exchange of information about cyberattacks, cyber incidents, and information security incidents were identified.

Keywords:
State Management, cybersecurity, mechanisms, information, Cyberattacks.

1. Introduction

The realities of the present indicate that cyber threats are evolving at an accelerated pace, cybercrimes are becoming more sophisticated, better organized, and transnational. This is due to the fact that the Internet, digital services, information, and communication technologies have become an integral part of the economy around the world: from electronic document management, online stores, and online banking to the Internet of things systems and intelligent enterprise management systems. With the growing dependence on the use of information and communication technologies in business and entrepreneurship, cyber risks and cyber threats grow accordingly, which requires a premature response to their prevention or solution and awareness of the risk factors of all stakeholders. A cybersecurity system must work in the public interest of both service providers and service users. It is the state, as the guarantor of the rights and freedoms of citizens, that should take responsibility for ensuring access to a stable, secure digital space that all citizens can use because ensuring an adequate level of cybersecurity is a necessary condition for the development of the information society.

The problem of effective cybersecurity requires a comprehensive solution and requires coordinated action at the national, regional, and international levels to prevent, prepare, respond and renew incidents by authorities, the private sector, and civil society. Taking into account modern socio-political and informational challenges of determining political, scientific, technical, organizational, and educational directions, designing an effective cyber defense system as part of a comprehensive response to cyber threats will contribute to the formation of an effective mechanism for countering threats in the cybersphere, which is ahead of the response to dynamic changes, the development and implementation of effective means and tools for a possible response to aggression in cyberspace, which can be used as a means of deterring military conflicts and threats in cyberspace.
The main purpose of the study is to determine the key aspects of the mechanisms of state management of the exchange of information about cyberattacks, cyber incidents, and information security incidents.

2. Methodology

To achieve this goal, we applied a number of theoretical methods that allowed us to form our own vision of the key aspects of the mechanisms of state management of information exchange regarding cyberattacks, cyber incidents, and information security incidents. These methods include a method of analysis and synthesis of information. The method of systematization of basic information on the chosen subject. The method of generalization and abstraction in the formation of relevant conclusions based on the results of the study. Our study is theoretical in nature, the main thing is to explore key

Manuscript received April 5, 2022
Manuscript revised April 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.4.5

aspects in the chosen topic and draw appropriate conclusions regarding the mechanisms of state management of the exchange of information regarding cyberattacks, cyber incidents, and information security incidents.

3. Research Results

Everyone feels how the world is changing lately. Industrial products, services, productivity, capital, knowledge, and information are in demand across borders and are exchanged in ever shorter time frames. This is due to the rapid development of information technology, the processes of formation and development of international cyberspace, which has been going on since the end of the twentieth century to this day. In the era of information technology, it is impossible to feel secure in cyberspace. With the development of technology, the number of crimes in this area is growing rapidly, so it can be said with confidence that it is "cybercrimes" in the 21st century that will be one of the most numerous. The emergence of new spheres of public life gives rise to new threats. State authorities, represented by law enforcement agencies, must respond to socially dangerous and illegal actions. Therefore, the need to ensure the security of the interests of a person and a citizen, society and the state, national interests in cyberspace is gradually gaining more weight and becoming one of the most important elements in ensuring the national security of the state. Cyberspace is limitless, and experienced hackers have all the necessary skills and tools to remain incognito in it. Today, cyber-attacks harm not only individuals and legal entities but also states. Cybersecurity is one of the key aspects of life in information times. Our smartphones, social networks, and other online fingerprints contain more information about users than they know about themselves. At the same time, they can be much more vulnerable to attacks by intruders than a person in real life. Therefore, all electronic information, services, and devices need protection and compliance with certain security rules [1-3].

Today we have a situation where global informatization actively controls the existence and life of the states of the world community, and information technologies are used at the highest levels of government in solving the problems of ensuring national, military, economic security, etc. At the same time, one of the fundamental consequences of the global informatization of state and military structures was the emergence of a fundamentally new environment for the coexistence and interaction of states - cyberspace. At the same time, it should be taken into account that cyberspace, although it has signs of an international one, does not have certain geographical features in the sense generally accepted in the world, it is characterized by the absence of borders, dynamics, and relative anonymity. The consequence of this was the transfer of the issue of cybersecurity from the level of information protection at a separate computer facility to the level of creating a unified state cybersecurity system as an integral part of the information and national security system responsible for protecting not only information in the narrow sense of the word but the entire cyberspace [4-6].

The essence of information security is to ensure the smooth operation of the organization and to minimize the damage from lurking security threats by preventing them and minimizing the consequences. Information security management allows you to share information while ensuring its protection and protection of computing resources. It is necessary to implement measures to detect and prevent the penetration of viruses into systems and procedures to inform users about their harm. Users should be reminded that preventing viruses is better than repairing the consequences of their entry. Virus protection must be based on high knowledge and understanding of security rules, and proper means of controlling access to systems. Should be used to check computers and storage media for known viruses, either as a preventative measure or as a routine procedure. Data change detection software should be installed on computers as necessary to detect changes in running programs.

For a long time, different companies have been analyzing the security of enterprises. They build models of various structures of commercial enterprises, financial institutions, banks, public institutions, educational institutions, and especially vulnerable enterprises of state importance. In different countries, work has begun on modeling objects and organizing attacks to further analyze the defeat of enterprises, financial structures, or important government institutions. For a long time, for 5-10 years, companies have been studying the influence of various factors on the development of threats in cyberspace. All of them were funded by individual companies that developed the cyber protection segment and state that used a lot of resources to create systems for monitoring, controlling, and checking security at the state level according to certain criteria that were identified as a threat to national security [7-8].

The protection of information today is, first of all, the protection of values. Modern society lives in an information environment where the creation, use, and dissemination of information is an important economic, political and cultural activity. Modern society is moving from the consumption and provision of economic services to economic information, which emphasizes information activities based on information technologies such as computers, mobile devices, and the Internet. Relationships

that arise in cyberspace are increasingly becoming the object of illegal encroachment. Information located in cyberspace can be used and attacked from a distance. Threats in cyberspace are as many and varied as cyberspace itself. They are inherent in the very nature of the network: their interconnectedness, scale, speed, and complexity of perception of what is happening - all these characterizes cases of cyberattacks.
There are a number of cyberattacks that are most popular today (Table 1).

Table 1: The main cyberattacks

№	*Cyberattacks*
1	Use of covert channels (information transfer paths that allow two processes to exchange it in a way that violates security policy)
2	The user performs some action that is outside the scope of his duties and violates the existing security policy, such as password disclosure
3	The attack can be carried out on the system as a whole; to data and programs contained on external (drives, network devices, terminals) or internal (RAM, processor) devices of the system, as well as in data transmission channels; processes and subprocesses of the system with the participation of users. The purpose of such attacks is either a direct impact on the operation of the process (its termination, changing privileges, and characteristics) or the opposite effect.
4	The user listens to the communication lines between two network nodes

States bear the legal, organizational and political responsibility for ensuring cybersecurity. Because cybersecurity and the protection of critical information and infrastructure are at the core of the security and prosperity of nations, security leadership must come from the highest levels of government. The government should define areas of responsibility and accountability, ensure control and continuity of all necessary actions. At the state level, this approach provides for a shared responsibility that requires coordinated action related to the prevention, response, and elimination of the consequences of all ministries and government agencies, as well as the private sector and citizens, to threats in the field of cybersecurity. At the regional and international level, this approach means coordination and cooperation with all major partners. And it is the governments of states that should provide a mechanism for training highly qualified personnel in the field of cybersecurity, capable of leading and coordinating this work.

Global informatization actively affects the functioning of the countries of the world society, information technologies are used in the process of solving the problems of ensuring state, military, and economic security. At the same time, one of the fundamental consequences of the global informatization of public and private structures was the emergence of a fundamentally new environment for confrontation between competitive states - cyberspace. The use of the Internet and information technology not only opens up endless opportunities for mankind but also creates new serious threats. More and more information is moving online, and at last count, there are already more than 20 billion devices connected to the Internet in the world, which is several times more than the population of the Earth. Also, billions of gigabytes of various information are collected on the servers. The world is becoming open, and such rapid growth requires the formation of "rules of the game" [9-10].

In an environment where cyber threats are constantly emerging and evolving, EU member states intend to pursue flexible, operational cyber security strategies when faced with new global threats. The cross-border nature of threats forces countries to enter into close international cooperation. Cooperation at the European level is necessary not only for effective preparation for cyber attacks but also for a timely response to them. A comprehensive government cybersecurity strategy is the first step on this path.

Modern forms of production are being reformatted for the online network in cooperation and interaction. For banking institutions, a key role in the use of provisions for action lies in the data on official information platforms. All official government destinations have their official web pages. Therefore, any attempts of cyber attacks and cyber aggression in a particular industry can create problems for the entire socio-political system as a whole. Such a progressive development of the information network requires the formation of specialists in the field of cybersecurity, who form a system of effective protection in various socially important areas. Therefore, using the example of the Ukrainian society, specialties related to cybersecurity and the IT industry are actively developing and leading the ratings of popular modern progressive professions with a high level of labor assessment and a shortage of qualified specialists. Of course, politics penetrates into all areas of social existence, since they all need political will and regulatory decisions, cyberspace in modern society is an important direction for improving the mechanisms of interaction between different users, for delineating the boundaries of permissible, tolerant, and correct statements, the boundaries of political and others. types of manipulations, features of the action of all these qualities on public acts and behavior.
Keyways to counteract cyberattacks at the government level should include the following (Fig. 1).

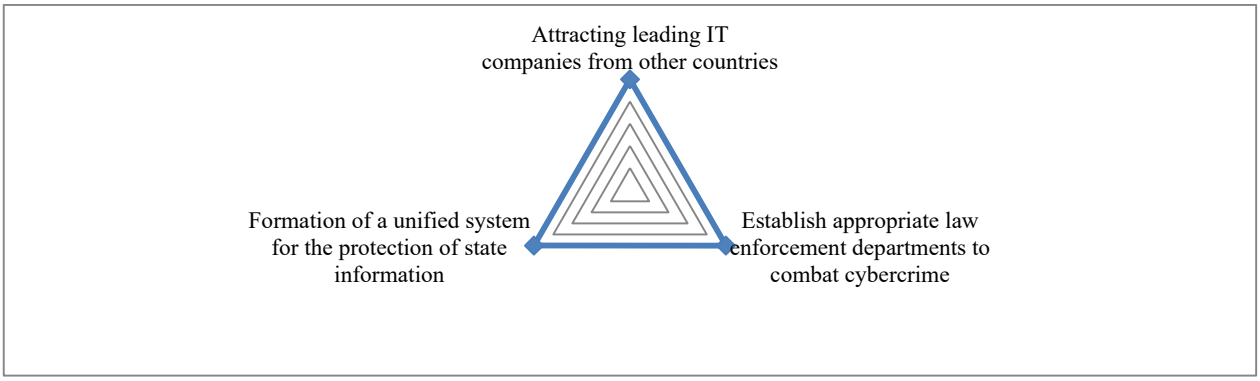

Fig. 1 Key ways to counteract cyberattacks at the government level.

When analyzing cybersecurity and its role in interaction in the information space for political actors who also use this space as a platform for confrontations and communication with citizens, one should take into account the normative component, the so-called legal, and the perception of political decisions in society (legitimacy), among ordinary citizens and politicians themselves, who also use information platforms and in a way that is specific to politicians, pursue their own political interests and receive public reaction as a response to political actions. It is this need that exists in the political plane, that is, taking into account both legality and legitimacy in the application of cybersecurity mechanisms as an innovative form of protection formed in the political plane. The subjects of politics become at the same time objects, which are also subject to the adopted political decisions in political activity, which gives such a process significance and publicity. After all, it is politicians who become a mirror for society in matters of the boundaries of what is permissible in the information space and the limits of the effectiveness of the current regulatory framework, the key to the formation of a legal, democratic, public society with a worthy political elite and political leaders who will become a model for the younger generation.

4. Discussions

Discussing the results of the study, it should be determined that the active development of the universality of communications, network convergence, the spread of mobile platforms, social networks, and remote applications have led to the fact that the concept of the protection perimeter is lost, as a result of which not only the threat landscape changes but also protection efforts are scattered, its efficiency decreases. At the same time, low-impact attackers have given way to modern cybercrime, sophisticated, well-funded, and capable of causing long-term disruption to businesses and government agencies. The attacks they implement have become not only less visible, longer in time, but also increasingly directional, capable of accumulating network resources to increase their range for the future.

Most protection systems are aimed at monitoring the network or end-devices and blocking malicious software at the entry point. These tools immediately scan files or network traffic for threats, usually using a signature-based method. If the malware is delivered to its destination in parts, or it is modified to become harmful after it enters the device, these detection technologies will no longer be able to notice the next attack deployment. At the same time, new attacks cannot be called momentary: they last a long time and require constant attention. That is, the traditional protection methods used by cyber defense units, whose only purpose is to detect and block attacks at the point of entry, are no longer effective [11-15].

The situational cyber defense center should not only respond to ongoing attacks but also take preventive measures to prevent cyberattacks and conduct processing and retrospective analysis of cyber incidents. In addition, when building a cyber defense center, it is necessary to take into account not only the stages of the implementation of cyberattacks but also the entire range of approaches to their analysis and synthesis, as well as the maximum arsenal of opportunities for other related activities.

The recent modern targeted attacks have shown the inability of standard means and methods of protection to resist them. This is because these tools are only focused on detecting and blocking attacks at the point of entry into the system.

5. Conclusions

Over the past two decades, digital technologies have developed rapidly. This caused a lot of excitement about the opportunities offered by the new era of digital gadgets. The transition from analog to digital technologies, that is, the era of the digital revolution, the prerequisites for which is the widespread use of information and communication technologies, has already begun and is progressing very actively. Increased digitalization and connectivity increase cyber security risks, thereby making society more vulnerable to cyber threats. At present, in the modern information society, computer crimes have become a characteristic feature of modernity.

Information, as a body of knowledge about actual data and the dependencies between them, has become a strategic resource, the basis for making any decision. Information systems created in state authorities and commercial structures circulate information containing secret information about the achieved potential in the field of economy, defense, science, and technology, confidential information about managerial, economic, commercial, financial, and other activities. Accordingly, information protection is a complex, knowledge-intensive, and multifaceted problem in the context of the introduction of modern information technologies, the creation of distributed computing systems, and communication networks, which is becoming especially acute.

The study of public-private partnerships in the field of information security should become promising in the future. Cybersecurity issues affect both the public and private sectors. A public-private partnership is a place where both sectors can collaborate and share methods to counter cyber threats. Attacks on a country's infrastructure can cause enormous damage to people's lives, services, and operations. Several models of successful partnerships in this area are exemplary throughout the world. The development of technology and the Internet responds to the growth of threats in cyberspace, constantly compromising data even in the most secure environments. Visible or covert threats are disadvantageous to an organization's information systems, assets, and data. Countries' critical infrastructures include telecommunications, electricity, energy, transportation, finance, operations, water, emergency services, food, health, chemicals, and classified materials. Most of the country's critical infrastructures operate through online technologies leading to positive economic development and gradual growth. Consequently, organizations and countries must collectively create systems to track and control critical infrastructure from invaders.

References

[1] Sylkin, O., Kryshtanovych, M., Bekh, Y., & Riabeka, O. 2020. Methodology of forming model for assessing the level financial security. Management Theory and Studies for Rural Business and Infrastructure Development, 42(3), 391-398. https://doi.org/10.15544/mts.2020.39 https://ejournals.vdu.lt/index.php/mtsrbid/index

[2] Kryshtanovych M., Dragan I., Chubinska N., Arkhireiska N., Storozhev R. 2022. Personnel Security System in the Context of Public Administration. IJCSNS International Journal of Computer Science and Network Security, Vol. 22 No. 1 pp. 248-254 https://doi.org/10.22937/IJCSNS.2022.22.1.34

[3] Kryshtanovych, M., Petrovskyi, P. ., Khomyshyn, I. . ., Bezena, I. ., & Serdechna, I. 2020. Peculiarities of implementing governance in the system of social security. Business, Management and Economics Engineering, 18(1), 142-156. https://doi.org/10.3846/bme.2020.12177

[4] Sylkin, O., Buhel, Y., Dombrovska, N., Martusenko, I., & Karaim, M. 2021. The Impact of the Crisis on the Socio-Economic System in a Post-Pandemic Society. Postmodern Openings, 12(1), 368-379. https://doi.org/10.18662/po/12.1/266

[5] Mohelska, H., & Sokolova, M. 2018. Management approaches for Industry 4.0 – the organizational culture perspective. Technological and Economic Development of Economy, 24(6), 2225-2240. https://doi.org/10.3846/tede.2018.6397

[6] Arnold, C., Kiel, D., & Voigt, K. I. 2016. How the industrial internet of things changes business models in diferent manufacturing industries. International Journal of Innovation Management, 20(08), 1640015. https://doi.org/10.1142/S1363919616400156

[7] Griffith, R., Huergo, E., Mairesse, J., & Peters, B. 2006. Innovation and productivity across four European countries. Oxford Review of Economic Policy, 22(4), 483-498. https://doi.org/10.1093/oxrep/grj028

[8] Mohelska, H., & Sokolova, M. 2016. Smart, connected products change a company's business strategy orientation. Applied Economics, 48(47), 4502-4509. https://doi.org/10.1080/00036846.2016.1158924

[9] Rennung, F., Luminosu, C. T., & Draghici, A. 2016. Service provision in the framework of Industry 4.0. Procedia - Social and Behavioral Sciences, 221, 372-377. https://doi.org/10.1016/j.sbspro.2016.05.127

[10] Shtangret, A., Korogod, N., Bilous, S., Hoi, N., & Ratushniak, Y. 2021. Management of Economic Security in the High-Tech Sector in the Context of Post-Pandemic Modernization. Postmodern Openings, 12(2), 535-552. https://doi.org/10.18662/po/12.2/323

[11] Voigt, K. I., Buliga, O., & Michl, K. 2017. Business model pioneers: how innovators successfully implement new business models. Cham: Springer. https://doi.org/10.1007/978-3-319-38845-8

[12] Zemplinerová, A., & Hromádková, E. 2012. Determinants of firm's innovation. Prague Economic Papers, 21(4), 487-503. https://doi.org/10.18267/j.pep.436

[13] Žižlavský, O. 2013. Past, present and future of the innovation process. International Journal of Engineering Business Management, 5(47), 1-8. https://doi.org/10.5772/56920

[14] Žižlavský, O. 2016. Innovation scorecard: conceptual performance measurement and management framework for innovation process. Journal of Global Business & Technology, 12(2), 10-27.

[15] Kryshtanovych, S., Bezena, I., Hoi, N., Kaminska, O., & Partyko, N. 2021. Modelling the assessment of influence of institutional factors on the learning process of future business managers. Management Theory and Studies for Rural Business and Infrastructure Development, 43(3), 363–372. Retrieved from https://ejournals.vdu.lt/index.php/mtsrbid/article/view/2352