Resilience and constantity of information infrastructure functioning within the national resilience system

Sergii Gnatiuk * [1 A]; Alexander Bakalynsky [2 A]; Danylo Myalkovsky [3 A]; Dmytro Pakholchenko [4 A]

***Corresponding author:** [1] Candidates of technical sciences, e-mail: sgnatuk30@gmail.com, ORCID: 0000-0002-1541-7058 -704X
[2] Candidates of technical sciences, e-mail: baov@meta.ua, ORCID: 0000-0001-9712-2036
[3] Candidate of Sciences of Public Administration, e-mail: daniilvm71@gmail.com, ORCID: 0000-0002-8246-8437
[4] Graduate student, e-mail: dimapakholchenko@gmail.com, ORCID: 0000-0002-6780-9459

[A] State Special Communications Administration, Kyiv, Ukrainia

Received: January 22, 2022 | Revised: March 20, 2022 | Accepted: March 31, 2022

DOI: 10.5281/zenodo.6385602

Abstract

The article examines the stability and resilience of the information infrastructure under the influence of modern cyber threats and cyber incidents. First of all, the importance of electronic communications in further implementation of programs and projects on informatization of all spheres and social processes in the framework of "e-society" and "e-government", as well as providing a wide range of public online services and online database access services was noted. ("ACTION"), online trade, services and works. Further digitalization and virtualization of all spheres of life and everyday life of the average citizen; processes of human-citizen-state relations and management systems, monitoring of critical infrastructure (at the object and general industry levels) increase the risks of cyber threats, which in turn affects the provision of a sufficient level of stability and resilience of all networks and systems. Today, experts distinguish such categories of crimes as: attempts to obtain user rights, attempts to obtain administrator rights, violations of corporate security policy and network malware. This mainly concerns the public and corporate sectors. As for the household level, it is mainly phishing, the purpose of which is to collect personal data for financial fraud, cyberbullying, etc. The events of January this year have shown that cyber threats are increasingly becoming an instrument of hybrid warfare. After all, as a result of cyber-attacks, the work of more than 24 websites of authorities and the "ACTION" platform was blocked and more than 70 sites were shut down to stop the spread of cyber-attacks. In addition, reports of mass mines in educational institutions in entire cities have become a new type of cyber threat. This allows us to talk about the need to increase the activity of the state and the private sector in combating cyber threats.

Thus, in the framework of building a national system of resilience, Ukraine took part in the exercise "Inviolable Resilience 2020", which was held under the auspices of NATO in Ukraine in September 2021 in Odessa. This provided practical experience: working in teams consisting of representatives of the security and defense forces and representatives of critical infrastructure; in the development of practical skills, abilities and competencies during the implementation of measures in crisis situations; elaboration of proposals on normative-legal regulation of raising the level of the national system of stability and cyber protection at all levels (from national to object).

Keywords: electronic communications, information infrastructure, cyber threats and cyber incidents, stability and resilience of the system.

Introduction

The current global trend is the spread of the results of the digital (Web 2.0) and industrial (4.0) revolutions, when the technologies of the Internet of Things, artificial intelligence, robots, SmartCity, etc. are beginning to be widely used. At the same time, cyberspace (virtual) is growing rapidly as physical space decreases. The leaders of such trends are social networks and social media. Also, all branches of government are moving to cyberspace. In addition, along with traditional spheres and sectors, digital ones are developing strongly, forming such new sectors as e-economy, e-business, e-banking, e education, telemedicine, e-services, etc. It should be noted that without a developed modern electronic communications network and the global Internet, it is problematic to build an "electronic society", "electronic government", "electronic society" and implement a "country in a smartphone". First of all, it requires a modern transport and communication infrastructure, which is an important component of the information infrastructure that forms the new "digital society". This course of events creates the preconditions for the emergence of new types of threats – cyber, the level of which increases in proportion to the level of digitalization, informatization and virtualization. Thus, with the growing impact of cyber threats on the stability and resilience of critical infrastructure in all spheres (economic, political, social and humanitarian) of society, the threat of increasing the number of crises affecting the national resilience system and national security in general.

Analysis of recent publications has shown that the acquisition of a high level of resilience of critical infrastructure in crisis situations deals with many modern researchers and scientists, among whom are such as: I. Zhilyaev, A. Kuzmich, A. Semenchenko, Y. Shchygol and others.

Despite the wide range of research, the issue of ensuring a high level of resilience of electronic communications infrastructure in crisis situations (during training and exercises) is part of the overall problem to which this article is devoted.

Formulation of tasks (goals) of the article. The aim of the article is to study measures to achieve a high level of sustainability of electronic communications infrastructure in crisis situations (during trainings and exercises).

Material and methods

The research methods used in the process of writing the article involve the use of general scientific and empirical techniques based on a systematic approach. In addition, general research methods such as generalization and comparison were used in the process. As a result of the analysis, the main range of problems for the stability and sustainability of the information infrastructure under the influence of cyber threats and cyber-attacks has been identified.

Results and discussion

Recent events have shown the vulnerability of modern information and telecommunication systems, information and communication resources, as well as automated control systems, automated information and analytical systems, cybercrime and cyber incident monitoring systems of various types and complexity. For example, "as a result of a cyber-attack in December 2016 on public financial institutions for almost three days was difficult to pay taxes and other payments to the budget, blocked the electronic system of tax administration, the work of customs was disrupted", "and as a result of the attack of the NotPetya virus on the computer systems of Ukrainian state and commercial institutions of Ukraine as of July 7, 2017, up to 10% of private, government and corporate computers were disabled" (Zhilyaev I., Semenchenko A., 2017).

The next example is the events that took place in January 2022 in our country, namely: "there was a massive cyber-attack on state information resources – one of the most powerful during the years of aggression. Almost 70 websites of central and regional authorities have been affected. Also, some sites, including the Action portal, were disabled together with administrators to avoid the possibility of spreading the attack to other resources" (Shchygol Y.). In view of the above, it can be noted that these cyber incidents bypassed the critical infrastructure of the energy sector (nuclear power plants, hydroelectric power plants), passenger transport (aviation, rail, subway). But you need to be prepared for the most serious scenarios.

After all, as A. Kuzmich emphasizes, “in the conditions of hybrid aggression of the Russian Federation cyberspace has finally become another theater of operations”, which is “sensitive and critical for both the individual and the state as a whole”, because “cyber-attack affects comfort (ability to pay, receive money, as well as electronic and physical services), security (for example, may affect the operation of process management systems), access to important information (work of government and business), as a consequence – the ability to manipulate people and society”, and therefore, “when a cyber-attack occurs, the enemy is not somewhere there, he is nearby, he sees the consequences of his actions and can quickly strike new blows” (Kuzmich A.). Thus, cyberspace becomes a new arena of hybrid confrontation between our country and the aggressor. The next element of cyberterror was mass reports of mines in public places in the city. Today, this is a new type of cybercrime, which is quite serious and requires considerable attention from the relevant government agencies and structures responsible for cybersecurity. This complicates not only the lives of ordinary citizens, but also affects the work of special units of the national police that respond to these challenges. But these are, so to speak, resonant types of cyber incidents (the “tip of the iceberg”), which are widely covered by the media. Cybercrime and cyber incidents are ongoing and involve not only public authorities and private big business, but also individual citizens. Digitalization and virtualization of many household processes leads to an increase in the number of consumers of digital services. First of all, it is: payment of wages and pensions on bank cards, online purchase / sale of goods and services and online payment for utilities. That is, cybercrime involving finances and personal data comes first. In view of the above, the load on electronic communications and information infrastructure is increasing, which requires a high level of stability and sustainability. The Operational Center for Cyber Incident Response of the State Center for Cyber Defense of the State Service for Special Communications and Information Protection provides a classification of cyber incidents into such categories as: “malicious (offensive) content; malicious code; collection of information by an attacker; attempts to intervene; intervention; violation of accessibility; violation of the properties of information; fraud; known vulnerability other” (Report on the work). As for the “categories of detection based on behavioral analysis”, their list is as follows: “scanning; violation of network security policy; data exfiltration; network worm; spam; connection to command and control servers; flood; DoS / DDoS; discrediting; anomaly in network behavior” (Report on the work). Thus, the tools of cybercriminals are quite broad and comprehensive. Thus, in 2021, the system of secure access of government agencies to the Internet blocked 39,361 attacks of various kinds; the system of detection of vulnerabilities and response to cyber incidents and cyber-attacks on the objects of monitoring recorded 503,353 suspicious events”, among which 8% of attempts to obtain user rights; attempts to obtain administrator rights – 12%; violations of corporate security policy – 53%; detection of network spyware – 19%” (EU4Digital). Also, according to the Government Computer Emergency Response Team of Ukraine (CERT-UA), “1,960 cyber incidents were registered and processed during this period” (EU4Digital). These figures show the seriousness of the problems that can cause cyber incidents not only to the state, but also to private business and ordinary citizens. It should also be borne in mind that the greatest danger to the national resilience system is the security of critical infrastructure in many sectors of the economy. According to the Law of Ukraine “On Critical Infrastructure”, critical infrastructure is considered as “a set of facilities that are strategically important for the economy and national security, the failure of which may harm vital national interests”, and therefore “violation or threat of staffing” the functioning of critical infrastructure or its individual object, the response to which requires the involvement of additional forces and resources” (On critical infrastructure). This should be prevented, as electronic communications are an important subject of information and telecommunications systems and automated control systems, monitoring and control of production processes in many sectors of the economy (energy, transport, water supply), where management is remote and not only, but also at the general level (Skybun O. Zh.). That is, the uninterrupted operation of the energy sector, railways, air transport, and subway operation depends entirely on the information infrastructure and electronic communications. That is why the effective provision of the national system of resilience should take place in "effective cooperation, coordination between civil and military structures" (The main task) in terms of public-private interaction. This is due to the fact that today a large percentage of the country's critical infrastructure is privately owned, and therefore ensuring a high level of resilience is possible only through close cooperation and interaction of government institutions dealing with cyber threats and private companies that own and users not only of information infrastructure, but also of critical infrastructure in general. It is also important to keep in mind that cyber threats and cybercrimes have no national borders, but are a global problem for all governments, society and private business. Therefore, we see a very effective format for combining the efforts of individual states, multinational companies and research centers in the fight against cybercrime. Only joint efforts can counter cyber threats and cyber incidents in the context of globalization of society and the globalization of cybercriminals themselves. At present, European countries within the European Union and NATO are taking various measures to prevent and combat cyber threats and cybercriminals. In addition, they involve countries that are just planning to join these organizations. For example, in the framework of the Eastern Partnership (further – EstP), which is an EU foreign policy initiative that extends to countries such as Azerbaijan, Belarus, Armenia, Georgia, Moldova and Ukraine. Thus, within the framework of this partnership, EU4Digital: Cybersecurity EstP activities are planned to strengthen national cybersecurity governance and the legal framework in the EstP; strengthening the protection of critical information infrastructure in the EstP; increase operational capacity to manage cybersecurity incidents in the EstP" (The main task), the main purpose of which is "to develop technical mechanisms and mechanisms for cooperation to strengthen cybersecurity and better preparedness for cyber-attacks in accordance with EU standards" (The main task). These activities should result in the "development of trust services in the digital economy and cybersecurity to increase the resilience of critical infrastructure as critical building blocks for compatible cross-border e-services in the Eastern Partnership region", which will ultimately increase "trust and security" (The main task). This can be achieved through institutional, legislative and regulatory support for cybersecurity and resilience at the national level of each country. In addition, Ukraine participates in practical activities, such as seminars, exchange of experience, training, etc. For example, in 2021, representatives of the state law enforcement agencies of Ukraine and NATO member states were involved in the weekly command and staff exercises "Inviolable Resilience 2020" (Specialists from the State Special Communications). Thus, for three days "50 participants from the teams of the State Special Communications Service, the Security Service of Ukraine, the National Bank, the Ministry of Defense and the Cyberpolice Department" live "competed on a virtual training ground with attackers played by Estonian specialized company CybExer Technologies OU" (Ukrainian security forces). The purpose of these competitions was to develop skills of "teamwork", effective communication and interaction of departments of various departments and companies with critical infrastructure "to ensure the resilience of our critical infrastructure and public information resources" (Ukrainian security forces; Bakalynskyi O., Pakholchenko D., 2021). Summing up the results of these exercises, Deputy Prime Minister for European and Euro-Atlantic Integration of Ukraine O. Stefanyshyna noted: "Ukraine is a very important partner of NATO and many members of the North Atlantic Alliance on issues related to combating hybrid threats. These exercises are the first element of national social resilience. And the results of today's exercises will be the basis for the implementation of the concept of resilience and further decisions of the Government, Parliament, President of Ukraine"

(Specialists from the State Special). These measures are a very important and valuable tool to increase the level of combat capability of domestic units to combat cyber threats. During such joint exercises there is the development of competencies (communicative, cyber, professional, etc.), adaptation in teamwork, acquisition and exchange of experience. The acquired practical experience and knowledge improve the level of preparation of both the legal framework in the field of cyber defense and national resilience, as well as the relevant plans for the implementation of measures for national resilience at the level of individual sectors of the economy and at the facility level. Therefore, a variety of practical measures will only improve the results of countering cyber threats and increase national resilience and sustainability at all levels.

Conclusions

In summary, today electronic communications and information infrastructure are the basis for the development of programs and projects “e-society”, “e-government”, “e-economy”, providing a wide range of public online services and online database access services (“ACTION”), online commerce, services and works. In addition, electronic communications and information infrastructure are critical infrastructure and affect the sustainability and resilience of the national economy, security and defense. Increasing the number of practical activities in the framework of multinational exercises will help increase the level of readiness to counteract both special government units and companies that own critical infrastructure facilities. In addition, the conducted exercises provide practical experience: in the work of joint teams of security and defense forces and business, which own critical infrastructure facilities; in the development of practical skills, abilities and competencies in combating cyber threats in crisis situations; making proposals for improving the regulatory and legal support of cyber protection of critical infrastructure and building a national system of resilience and at all levels (from national to site).

Given the constant growth of digitalization and informatization of social processes, the issue of cyber threats (cyber protection) and resilience will not lose relevance, and therefore the demand for further intelligence will only increase.

References

[1] EU4Digital: 4 Cybersecurity East. Available from : https://eufordigital.eu/en/discover-eu/eu4digital-improving-cyber-resilience-in-the-eastern-partnership-countries/. (Date of application 24.01.2022).

[2] The main task of cyber training is to develop effective mechanisms and skills to ensure the cyber resilience of critical infrastructure and public information resources. Available from : https://cip.gov.ua/ua/news/golovne-zavdannya-kibernavchan-napracyuvati-efektivni-mekhanizmi-i-navichki-dlya-zabezpechennya-kiberstiikosti-kritichnoyi-infrastrukturi-ta-derzhavnikh-informaciini (Date of application 24.01.2022).

[3] Zhilyaev I., Semenchenko A. (2017). Organizational and legal mechanisms of development of the national cybersecurity system of Ukraine: Status and prospects. *Strategic Priorities*, № 4 (45), PP. 55-63.

[4] Report on the work of the system for detecting vulnerabilities and responding to cyber incidents and cyber-attacks for 2021. Operational Center for Cyber Incident Response of the State Center for Cyber Defense of the State Service for Special Communications and Information Protection. Available from : https://cert.gov.ua/article/17696

[5] Kuzmich A. The reality of cyber warfare. What lessons have we learned from the large-scale hacker attack on Ukraine. Available from : The reality of cyber warfare. What lessons have we learned from the large-scale hacker attack on Ukraine (cip.gov.ua). Date of application 24.01.2022).

[6] On critical infrastructure: the law of Ukraine Voice of Ukraine of 14.12.2021 – № 236.

[7] Ukrainian security forces together with NATO representatives completed the exercise "Inviolable Sustainability 2020". Available from : https://m.day.kyiv.ua/uk/ news/180921-ukrayinski-sylovyky-spilno-z-predstavnykamy-nato-zavershyly-navchannya-neporushna. (Date of application 23.01.2022).

[8] Specialists from the State Special Communications from September 15 to 21, 2021 blocked more than 39 thousand attacks on state information resources. Available from : https://cip.gov.ua/en/news/fakhivci-derzhspeczv-yazku-z-15-po-21-veresnya2021-roku-zablokuvali-bilshe-39-tisyachi-atak-na-derzhavni- information resource. (Date of application 24.09.2021).

[9] Shchygol Y. Specialists of the State Special Service are investigating a cyber attack on the websites of government agencies to understand the whole chain of its implementation. URL: Yuri Shchygol: specialists of the State Special Communications Service are investigating a cyber attack on the websites of state bodies to understand the whole chain of its implementation (cip.gov.ua). (Date of application 24.01.2022).

[10] Bakalynskyi O., Pakholchenko D. (2021), "Analysis of cybersecurity requirements of automated process control systems as critical information infrastructure", Èlektronnoemodelirovanie, Vol. 43, № 4, pp.103-112. DOI :10.15407/emodel.43.04.103

[11] Skybun O. Zh. The influence of cyber threats on the functioning of electronic communications (telecommunications) in conditions of building a "digital state". Visn. NADU. Seriia "Derzhavne upravlinnia". 2020. № 4 (99). P.84-92.