Teka of Political Science and International Relations – UMCS, 2019, 14/2, 119–137
DOI: 10.17951/teka.2019.14.2.119-137

COMPARISON OF THE POLISH AND UKRAINIAN CYBERSECURITY SYSTEMS

Viktoria Boiko
National Institute for Strategic Studies, Kyiv
ORCID: https://orcid.org/0000-0002-7546-9909
e-mail: vboiko@niss.gov.ua

Abstract: Ensuring information security is a challenge in the new COVID-19 home office reality that is essential to be expanded in its tackling across the national borders, throughout the national cybersecurity systems, across the entities that form the national cybersecurity system, i.e. business entities providing services using ICT systems, users, public authorities, and specialised entities dealing with ICT security at the operational level in different countries.
As a number of researchers outline in their findings, any significant disruption to the functioning of the information and cyberspace, whether global or local, has an impact on security and safety across borders, the efficiency of public sector institutions, production and service processes, and ultimately on national, community, but also personal security [Anderson, Hern 1996; Buzan, Wæver, de Wilde 1998; Deibert 2002; Hansen, Nissenbaum 2009; Świątkowska 2012].
The purpose of this article is to have a closer look at the operational framework of governmental structures responsible for the assurance of cybersecurity in Poland and in Ukraine. Poland's example is important as it is closely linked to the cybersecurity frameworks of NATO, the EU, UN and OSCE. This cooperation plays an important role in the fight against the increasing number of incidents. Meanwhile, Ukraine is preparing to become a member of the pan-European and transatlantic information and cybersecurity networks, i.e. it is important to have a thorough understanding of the cybersecurity system and its bottlenecks.

Keywords: cybersecurity, information security, ENISA, framework of cybersecurity policy

INTRODUCTION. LEGISLATIVE CONTEXT OF THE POLISH CYBERSECURITY SYSTEM

The National Framework of Cybersecurity Policy of the Republic of Poland for 2017–2022 is a strategic document that describes actions that are to be taken by the governmental administration, aimed at raising the level of cybersecurity in the Republic of Poland, including the Policy for the Protection of Cyberspace of the Republic of Poland.

On August 1, 2018, the President of the Republic of Poland signed the Act on the National Cyber Security System, implementing in the Polish legal system the Directive of the European Parliament and of the Council on measures for the overall security of network and information systems in the Union (Directive 2016/1148 – NIS Directive). Poland completed the implementation of the NIS Directive on November 21, 2018 [Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa…]. The purpose of the National Cybersecurity Act, prepared by the Ministry of Digitalization, was to develop legislation to implement the NIS Directive and create an effective ICT security system at the national level.

The system includes key service operators (e.g. energy, transport, healthcare and banking), digital service providers, CSIRTs (National Security Response Team) at the national level, as well as industry cybersecurity teams, organizations providing cybersecurity services, cybersecurity authorities, and a single point of contact for communication in the framework of cooperation in the European Union in the field of cybersecurity. Operators of essential services are required to take effective security measures, assess cyber security risks, as well as report major incidents and cooperate with national CSIRTs.

Public administration bodies as well as telecommunications companies are also included in the national cybersecurity system. Cybersecurity requirements also cover digital service providers, i.e. commercial Internet sites, cloud technologies and search engines. Due to the international specificity of these entities, obligations towards digital service providers are subject to a regulatory regime agreed at the EU level. Political and strategic responsibility for cybersecurity is shared between the bodies responsible for strategic management, the Ministry of Digitalization and the Ministry of Defense. Some decision-making competencies are also shared between other ministries, agencies and government agencies.

The Ministry of Digitalization is a key organization responsible for the protection of cyberspace, the process is overseen by the Council of Ministers [Ministerstwo Cyfryzacji…]. The Ministry should fulfill its obligations with the assistance of a special interdepartmental group appointed by the Prime Minister, the role of this body is to implement general policies and make proposals for further action aimed at implementing the digital policy of the state.

The Ministry also supports the Council for Digitalization (*Rada do Spraw Cyfryzacji*, RC) in making strategic decisions [Rada do Spraw Cyfryzacji…]. The Council provides analytical support to the Ministry as well as to the Committee of the Council of Ministers for Digitalization, supports the development of the information society, prepares draft decisions, or legislative initiatives. The Council is formed by the Ministry and consists of representatives of the Ministry, but also acts as a multilateral forum for cooperation between stakeholders on the Polish digitalization agenda.

As the main goal of the Council is to act comprehensively and transparently, the selection of members of the Council takes into account primarily the factor of representing the interests of various parties interested in the digitalization of

the state, among government agencies, local authorities, entrepreneurs, academia, technical experts and NGOs.

According to Art. 17 item 10 of the Law on Computerization of the Activities of Entities Performing Public Tasks, the minister authorized to deal with the questions of digitalization appoints members of the Board for two-year terms from among the recommended candidates [Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne…].

In accordance with para. 17 of Art. 10 of the above law, the Minister of Digitalization determines, by issuing a relevant resolution, the amount of remuneration of a member of the Board for participation in meetings, taking into account the functions performed by a member of the Board and the scope of duties of a member of the Board, taking into account the minimum wage determined on the basis of the Law as of October 10, 2002 as the minimum wage that was in force on the day of the appointment of the Council [Ustawa z dnia 19 lipca 2019 r. o zmianie ustawy o minimalnym wynagrodzeniu za pracę…].

In accordance with para. 18 of the law, non-local members of the Council are entitled to additional daily payments and reimbursement of travel and accommodation expenses under the conditions specified in the provisions of Art. 775 para. 2 of the Law of 26 June 1974 – Labor Code [Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 16 maja 2019 r. w sprawie ogłoszenia jednolitego tekstu ustawy – Kodeks pracy…]. In item 19 of the Law, the detailed mode of work of the Council is defined in its regulations established at the request of the Council by the Minister of Digitalization. Working on a number of issues, the Council may set up *ad hoc* working groups, which may include representatives of the state and the private sector, as well as of the non-governmental sector, and all stakeholders. For example, the decision adopted at the meeting of the Digitalization Council on March 14, 2019 established the following working groups:

- working group on infrastructure (including digital highways, government cloud technology, state information architecture),
- working group on digital competencies (including competencies of the future),
- working group on public electronic services (including electronic delivery, digitalization of health care),
- working group devoted to issues of artificial intelligence,
- cybersecurity working group (including data security),
- technology working group (including 5G, Internet of Things, blockchain).

The Cyber Security Department of the Ministry of Digitalization, established in 2015, performs tasks related to the coordination of cybersecurity issues [Cyber Security Department…]. The main tasks of the Department are: development and implementation of strategic documents and regulations in the field of cybersecurity; national and international cooperation (in particular, with the institutions of the European Union); development of guidelines and standards for appropriate measures to protect IT systems; preparation of cybersecurity analyses and related

risks to national security; and development of central curricula, cyberlearning and tests. The Department cooperates with universities, institutes, public organizations and the private sector. As the Ministry oversees the Scientific and Academic Computer Network (*Naukowa Akademicka Sieć Komputerowa*, NASK), all tasks related to this function are also performed by the Department.

National Cybersecurity Center (*Narodowe Centrum Cyberbezpieczeństwa*, NC Cyber) focuses on educational and research goals, ensuring the reliability and efficiency of ICT networks.

The National Security Bureau (*Biuro Bezpieczeństwa Narodowego*) provides guidance on strategic actions and decisions in the field of cybersecurity. The doctrine is not a legally binding document, but rather shapes the political and strategic approach to cybersecurity in Poland.

The Department of Law and Non-Military Security (*Departament Prawa i Bezpieczeństwa Pozamilitarnego*) is responsible for cybersecurity. There is also a special team for the protection of cyberspace, consisting of representatives of the National Security Bureau and external experts who are responsible for updating the Doctrine.

Other government agencies with core responsibilities for cybersecurity management are:

- The Ministry of Justice (*Ministerstwo Sprawiedliwości*, MS), which creates the law on cybercrime and oversees its proper implementation,
- The Ministry of the Interior and Administration (*Ministerstwo Spraw Wewnętrznych i Administracji*, MSWiA) – monitors police actions in the fight against cybercrime and is responsible for crisis management, oversees the National Police Headquarters. The latter is responsible for the fight against cybercrime within the structure of the Criminal Investigation Bureau,
- The Internal Security Agency (*Agencja Bezpieczeństwa Wewnętrznego*, ABW) is a government agency that protects the internal security of Poland and its citizens, including the implementation of IT security tasks related to the processing of confidential data,
- The Government Security Center (*Rządowe Centrum Bezpieczeństwa*, RCB) is an institution accountable to the Prime Minister that is involved in crisis management at the governmental level. It plays a key role in building a Critical Infrastructure Security (CI) system in Poland, including the cybersecurity aspect. The Director of the Center, together with ministers and heads of individual central agencies, prepares lists of domestic and European critical infrastructure and maintains the National Critical Infrastructure Security Program,
- Office of Electronic Communications (*Urząd Komunikacji Elektronicznej*, UKE) – a regulator of the telecommunications market, controlled by the Ministry of Digital Affairs, which ensures the implementation of the Law on Telecommunications in the context of cyberspace, and receives information on security incidents and the integrity of telecommunications

networks from network and telecommunications service providers and sends them, *inter alia*, to ENISA,
- The Financial Supervision Commission (*Komisja Nadzoru Finansowego*, KNF) is a financial regulator that provides advice on the management of information technology and environmental security of ICTs in banks,
- The Inspector General for Personal Data Protection (*Generalny Inspektor Ochrony Danych Osobowych*, GIODO) is a state body authorized to monitor the compliance of data processing with the provisions on personal data protection, issue administrative decisions and consider complaints regarding the implementation of personal data protection provisions, issue opinions on draft laws and regulations, protect personal data, initiate and take measures to improve the protection of personal data.

CERT / CSIRT / SOC SYSTEM

The tasks of the minister responsible for digitalization include: development of the Cybersecurity Strategy, information policy on the functioning of the national cybersecurity system, reporting to EU institutions and introduction, from January 1, 2021, of an ICT system to automate incident reporting and processing, assessment ICT risks and cyber threat warnings.

CSIRT teams at the national level will work together to ensure a comprehensive and complete cybersecurity risk management and incident response system, including in particular serious and critical cases, *inter alia*, the threat to the interests of the state. One of the main tasks of CSIRT NASK, CSIRT GOV and CSIRT MON is to coordinate the analysis and respond to reported incidents: In case of CSIRT NASK, these are local self-government units, budgetary institutions of local self-government, executive bodies, institutions of budgetary economy, state universities and the Polish Academy of Sciences, Department of Technical Inspection, Polish Air Navigation Services Agency, Polish Accreditation Center, National Fund for Environmental Protection and Water Management and Regional Funds for Environmental Protection and Water Management, commercial companies that perform utility tasks aimed at constantly meeting the needs of the population, citizens.

In case of CIRT GOV, these are public authorities, including public administration bodies, state control and law enforcement bodies, as well as courts and tribunals, Social Insurance Institution (*Zakład Ubezpieczeń Społecznych*, ZUS), Agricultural Social Insurance Fund (*Kasa Rolniczego Ubezpieczenia Społecznego*, KRUS), National Health Fund (*Narodowy Fundusz Zdrowia*, NFZ), National Bank of Poland (*Narodowy Bank Polski*, NBP), etc.

CSIRT MON – entities that report to or are controlled by the Minister of National Defense, including the structures of the ICT system or ICT network. Those entities are covered by a single list of facilities, devices and services that are part of

the critical infrastructure; entrepreneurs who are owners of objects of economic or defense significance, for which the Minister of National Defense is the body that organizes and controls the implementation of tasks for the protection of the state.

The law [Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa…] also defines cybersecurity authorities responsible for overseeing operators of basic services and digital services. Operators of key services are required to take effective security measures, assess cyber security risks, provide information on serious incidents and address them in collaboration with CSIRT at the national level.

The tasks of the relevant competent authority are:

- to conduct ongoing analysis of entities in a particular sector or sub-sector in terms of their recognition as a key service operator,
- to decide on the recognition of the business entity as the operator of the key service,
- to prepare recommendations for actions aimed at strengthening cybersecurity, including sectoral recommendations on countering incidents (cooperation with CSIRT NASK, CSIRT GOV, CSIRT MON and sectoral cybersecurity teams),
- to inspect key service operators and digital service providers (monitoring compliance with the provisions of the Law),
- at the request of CSIRT NASK, CSIRT GOV or CSIRT MON, to appeal to key service operators or digital service providers within a specified period to resolve vulnerabilities that have caused or may lead to a serious, significant or critical incident,
- to participate in cybersecurity exercises organized in the Republic of Poland or the EU,
- to establish a sectoral cybersecurity team for the sector or subsector as needed.

COLLEGIUM OF CYBERSECURITY

The Collegium [*Powstaje Kolegium ds. Cyberbezpieczeństwa…*] is an advisory body on cybersecurity and the activities of CSIRT MON, CSIRT NASK, CSIRT GOV, sectoral response teams and competent authorities. The Collegium consists of: Prime Minister, Minister of Computerization, Minister of National Defense, Minister of Foreign Affairs, Head of the Prime Minister's Office, Head of the National Security Bureau, if appointed by the President of the Republic of Poland, a Minister member of the Council of Ministers authorized to coordinate intelligence services, or the person authorized by him.

The Director of the Government Security Center, the Head of the Internal Security Agency or his Deputy, the Head of the Military Counterintelligence Service or his Deputy, and the Director of the Scientific and Academic Computer

Network [Naukowa i Akademicka Sieć Komputerowa…] (a national research institute) attend the discussions within the Collegium Board.

Among the tasks of the Collegium there can be distinguished: providing opinions on recommendations and plans to combat cybersecurity threats; conducting by CSIRT MON, CSIRT NASK, CSIRT GOV, industry response teams and competent authorities of the tasks assigned to them in accordance with the instructions and plans to combat cybersecurity threats; coordination of cooperation between the bodies that manage or control CSIRT MON, CSIRT GOV and CSIRT NASK; organization of exchange of information concerning cybersecurity and the international position of the Republic of Poland between public administration bodies.

DEVELOPMENT OF THE STRATEGIC AND LEGAL BASIS OF THE POLISH CYBERSECURITY SYSTEM

The Cybersecurity Strategy of the Republic of Poland for 2019–2024 as a continuation and extension of actions taken by the government administration to increase the level of cybersecurity in the Republic of Poland supersedes the National Framework of Cybersecurity of the Republic of Poland for 2017–2022. The Strategy foresees that the Republic of Poland shall actively participate in the work on establishing European cybersecurity certification schemes in accordance with Regulation (EU) No. 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act).

Actions at the national level shall include: 1) designation of the national cybersecurity certification authority that is to issue European cybersecurity certificates, 2) overseeing national conformity assessment bodies which assess compliance of products, services and processes with the requirements set forth in the European cybersecurity certification schemes, 3) cooperation with the national accreditation body – the Polish Centre for Accreditation – in order to monitor and supervise activities of the accredited conformity assessment bodies which are to assess compliance with Regulation (EU) No. 2019/881 of the European Parliament and of the Council.

The Ministry of Digitalization of Poland has also recently initiated an amendment to the law on the national cybersecurity system in view of changes in the field of cyberspace at the European level. One of the reasons was the emergence of the European Code of Electronic Communications [Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast)] which allows, among other things, the standardization of cyber incident reporting procedures at the national level. At the same time, the European Commission emphasizes the need to ensure the security of next-generation broadband, i.e. 5G technology.

The law also lacked harmonization at the national level of incident reporting procedures, which should also be reported by telecommunications companies. The amendments to the law provide for the creation of conditions for the initiation of computer incident response teams (CSIRTs) in sectors and sub-sectors of the economy that are key to the socio-economic security of the state (sectoral CSIRTs). It is also envisaged that key service operators will work with competent authorities and national CSIRTs in the sector to exchange information on incidents, vulnerabilities, threats and best practices. The possibility of creating centers of analysis and exchange of information (ISAC) was also mentioned.

In the new law, the Collegium of Cybersecurity [*Powstaje*...] should be empowered to assess the risks borne by suppliers of equipment and software related to cybersecurity of the subjects of the national cybersecurity system [Rozporządzenie Rady Ministrów z dnia 2 października 2018 r. w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa…]. Such risk assessments made by EU Member States have been agreed with the European Commission and ENISA as one of the strategic measures in the 5G Toolbox.

Amendments to the law provide for more dynamic processes of creating sectoral CSIRTs in all sectors of the economy, which are key to the socio-economic security of the state and citizens. The establishment and operation of ISACs – specialized organizations, through which cybersecurity actors will be able to constantly share information on incidents, threats, vulnerabilities and best practices – is also envisaged [Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa 2020].

KEY TAKEAWAYS ON THE POLISH CYBERSECURITY SYSTEM

A three-track national cyber incident response system has been established with the following responsibilities: the first level of coordination is the level of the Ministry of Digitization; the second level is the level of response to incidents which includes civilian and military components: a) the Government Cyber Incident Response Team (CERT.GOV.PL) acts as the main CERT in the field of emergency response within government capabilities and civilian response, coordinates the processes of joint response to computer incidents in cyberspace. The team was established in 2008 and works within the structures of the Internal Security Agency. CERT.GOV.PL deals with all users of ICT systems within the public sector (with the .gov.pl domain name) and businesses that make up the critical ICT infrastructure of the state; b) the Polish Military Computer Incident Response Team (MIL-CERT.PL). The third level of implementation refers to administrators responsible for individual ICT systems.

Crisis management in Poland is divided into four stages: prevention, preparation, response and reconstruction. According to the Law of April 26, 2007 on Crisis Management and the updated National Crisis Management Plan 2013/2015,

the Head of the Internal Security Agency is responsible for crisis management and protection of critical infrastructure and countering threats in cyberspace.

The prevention phase requires the involvement and cooperation of numerous central and local government structures, and is assisted by a number of ancillary institutions. During the prevention phase, the head of the Internal Security Agency (through CERT.GOV.PL and the IT Security Department) performs tasks which include the protection of classified information, accreditation of classified information processing systems, as well as security expertise and assessment as part of the certification process. Its tasks also include raising awareness and knowledge of government officials about cyber threats, developing the capacity of government departments to protect against cyber threats, creating catalogs of threats and potential vulnerabilities, and preparing guidelines and instructions for public administration. The Agency also acts as a national coordinator for NATO's cybersecurity policy. The Ministry of the Interior and Administration, the Ministry of Digitalization, the Ministry of Defense, the Government Security Center, the Council of Ministers and regional officials are involved in the preparatory phase.

As regards the Internal Security Agency, this phase includes the issuance of ICT security recommendations, ICT security training for public administration IT system administrators, security tests, the development of an early warning system against cyber threats, and the implementation and support of prevention solutions. During the response phase, the head of the Internal Security Agency is responsible for coordinating the process of reviewing computer incidents in the state administration, detecting, recognizing and combating cyber threats, providing information to administrators when detecting errors in IT systems, handling incidents in networks covered by ARAKIS-GOV., publication of warnings and alerts, post-violation analysis and preparation of recommendations aimed at improving the security of public ICT systems. The supporting institutions at this stage are: the Ministry of the Interior and Administration, the Ministry of Digitalization, the Ministry of Defense, the Government Security Center, the President of the Republic of Poland, the Council of Ministers, and the Voivode.

During the reconstruction phase, in which CERT.GOV.PL is responsible for post-incident analysis, the supporting institutions are: the Ministry of the Interior and Administration, the Ministry of Defense, the Foreign Intelligence Agency, the Government Security Center and regional officials. At the same time, Poland's cybersecurity system is multilevel and is actively trying to involve non-governmental structures. For example, in 2016, the national grid operator Polskie Sieci Elektroenergetyczne (PSE) signed an agreement with the NATO Center for Excellence in Energy Security, outlining cooperation in the field of critical infrastructure protection. Cybersecurity was one of the central points of the agreement, PSE was the first Polish company to establish this type of cooperation and can serve as an example of a bottom-up initiative that promotes the development of national cyber systems.

It is also worth noting the examples of *pro bono* activities of the public organization Polish Civil Cyber Defense (*Polska Obywatelska Cyberobrona*), whose

activities were launched in 2015. The aim of the association is to bring together cybersecurity experts who are ready to promote national security in the event of an incident free of charge.

LEGAL AND ORGANIZATIONAL FRAMEWORK OF THE UKRAINIAN CYBERSECURITY SYSTEM

The process of developing an effective cybersecurity system was started in Ukraine in 2014. The key impetus for building a cybersecurity system in Ukraine came from power grid cyberattacks which took place on 23 December 2015 and is considered to be the first known successful cyberattack on a power plant. Hackers were able to successfully compromise information systems of three energy distribution companies in Ukraine and temporarily disrupt electricity supply to the end consumers [Park, Walstrom 2017].

In 2016, the Cybersecurity Strategy of Ukraine was approved, where it was first recognized at the legislative level the urgent need to create a national system of cybersecurity as a component of the system of ensuring national security of Ukraine, which, above all, had to ensure interaction on the issues of cybersecurity of major actors – state bodies, local authorities, military formations, law enforcement agencies, scientific institutions, educational institutions, non-governmental organizations and business [Decree of the President of Ukraine of 27 January 2016 On the Decision of the National Security and Defense Council of Ukraine "On the Cyber Security Strategy of Ukraine"].

The Strategy of Cybersecurity of Ukraine provided the basis for the development of further regulations on cybersecurity issues. It defined the main cyber threats to Ukraine, outlined the priorities and directions of state policy in this area and identified the main state bodies responsible for cybersecurity and their functions. This legal document has become the basis for systematic action to build the National Cyber Security System (NCSS). The provisions of the Strategy have been further developed in the Law of Ukraine "On Basics of Providing Cyber Security of Ukraine" (Cyber Security Law), adopted by Ukraine's Parliament (Verkhovna Rada of Ukraine) on 5 October 2017.

The law formalized the model of the NCSS, announced in the Cybersecurity Strategy of Ukraine, defining it as "a set of actors providing cybersecurity and interrelated measures of political, scientific, technical, informational, educational character, organizational, legal, operative, intelligence, counter-intelligence, defense, engineering and technical measures, as well as measures of cryptographic and technical protection of national information resources, cyber defense of critical infrastructure" [Law of Ukraine "On Basics of Providing Cyber Security of Ukraine" 2017].

The other legal documents that form the basis for cybersecurity legislation in Ukraine are the following: The Constitution of Ukraine; National Security Strategy of Ukraine; Law on National Security; Law on Information; Law on

Information Protection in Information and Telecommunication Systems; Law on Telecommunications; Law on Protection of Personal Data; other laws, as well as statutory legal acts issued in accordance with these laws.

The mechanisms of interdepartmental interaction and coordination as well as public-private partnership in the cyber security domain have been established. A number of measures have been taken to increase capabilities of main state bodies, responsible for cybersecurity. International partnership in the sphere of cybersecurity has been reinvigorated, namely the NATO Trust Fund on Cyber Defence for Ukraine has been founded, aimed at helping Ukraine to develop capabilities to counter cyber threats.

At present, the main problematic issues that hamper further development of the NCSS of Ukraine are the lack of effective cybersecurity policy implementation, low level of cyber-risk awareness and insufficient human capacity of the main actors of the NCSS. Among other problems there are absence of legal and organizational framework for critical infrastructure protection, outdated standards for cybersecurity, weak national legislation on cybercrime and necessity to facilitate public-private partnership.

THE STRUCTURE OF THE NCSS OF UKRAINE

The main actors of the NCSS are the following: the State Service for Special Communications and Information Protection of Ukraine, the National Police of Ukraine, the Security Service of Ukraine, the Ministry of Defense of Ukraine and the General Staff of the Armed Forces of Ukraine, intelligence agencies, the National Bank of Ukraine. Coordination and control of the activities of the security and defense sector entities that provide cybersecurity of Ukraine is carried out by the National Security and Defense Council of Ukraine (NSDC) through the subsidiary body, the National Coordinational Cyber Security Center.

The State Service for Special Communications and Information Protection of Ukraine – this organization provides such functions as:

- development and implementation of state policy on the protection in cyberspace of governmental information resources and information, the requirement for protection of which is established by law, cyber protection of critical infrastructure,
- coordination of the activities of other cybersecurity entities regarding cyber protection, exercise state control in this area,
- ensuring the creation and operation of the National Telecommunication Network, implementation of organizational and technical model of cyber protection,
- carrying out organizational and technical measures to prevent, detect and respond to cyber incidents and cyberattacks and to eliminate their consequences,

- informing about cyber threats and appropriate methods of protection against them,
- coordinating, organizing and conducting critical infrastructure vulnerability audits,
- ensuring the functioning of the State Center for Cyber Protection and the Government Response Team for Computer Emergencies in Ukraine (CERT-UA).

An important role in cyber protection of the state information resources, detection and counteraction to cyberattacks and cyber incidents is being played by the State Center for Cyber Protection and Countering Cyber Threats (SCCPCC) created on July 1, 2015 as a structural unit of the State Service for Special Communications and Information Protection of Ukraine. Creation of the mentioned Center has become an important step towards the development of the National Cybersecurity System in Ukraine. Among the main tasks there can be distinguished: assessment of the state of information protection in governmental authorities; ensuring the long-term functioning, security and development of the National Confidential Communication System; ensuring the functioning and development of the antivirus protection system for state authorities; ensuring the functioning and modernization of the System of Secured Internet Access for the state authorities of Ukraine and the Secured Internet Access Point of the State Service for Special Communications and Information Protection of Ukraine.

The main task of the Center is to ensure the functioning of the Emergency Response Team of Ukraine (CERT-UA), which is its structural subdivision. The unit was established in 2007. In 2009, it was accredited to the Forum in Incident Response and Security Teams (FIRST) [*CERT-UA: skoraya kiberpomosht'* 2014]. Functional tasks of CERT-UA involve accumulation and analysis of data on cyber incidents, maintenance of the state register of cyber incidents and providing state bodies and private owners of critical infrastructure with practical help in preventing, detecting and eliminating the effects of cyber incidents. What is more, CERT-UA organizes and conducts practical workshops on cyber protection as well as interacts with law enforcement agencies, foreign and international organizations on responding to cyber incidents.

In addition, the Emergency Response Team of Ukraine provides the operation of a number of services available on its official website: accumulation and processing of information about the compromised IP-addresses; active monitoring of network threats; service for verifying vulnerabilities; functioning of on-line platform for reporting a cyberincident [Emergency Response Team of Ukraine. *Skorystaytesya nashoyu dopomohoyu v likvidatsiyi kiberzahroz*]. The CERT-UA plays an important role in the NCSS as a practical unit that responds directly to a cyberattack, helps to restore network functioning and eliminate negative impacts of cyber incidents. The most prominent examples of CERT-UA activity are the elimination of hacker attacks on the automated system "Elections" during the extraordinary presidential elections in Ukraine in 2014, the localization and

neutralization of the BlackEnergy virus on the objects of the energy and transport complex of Ukraine in 2015 and 2016. The CERT-UA team together with specialists from Cyber Policies, the Security Service of Ukraine, foreign partners, and private sector participated in counteracting and eliminating the consequences of largescale hacker attacks against Ukraine in June 2017. On February 2, 2018, a new unit – the Cyber Threat Response Center (CTRC) – was established within the State Center of Cyber Protection and Countering Cyber Threats. This unit is engaged primarily in providing cyber protection of state authorities and critical information infrastructure of Ukraine [Emergency Response Team of Ukraine. *Vidkryttya Tsentru reahuvannya na kiberzahrozy*].

The Security Service of Ukraine (SSU) – this organization carries out the following tasks: to prevent, detect, suppress and disclose crimes against peace and security of mankind committed in cyberspace; to carry out counter-intelligence, operational and investigative activities aimed at combating cyberterrorism and cyberespionage; to secretly check readiness of critical infrastructure for possible cyberattacks and cyber incidents; to counteract cybercrime, the consequences of which can create a threat to the vital interests of the state; to investigate cyber incidents and cyberattacks concerning the state electronic information resources, the information protection, the requirements of which are established by law, critical infrastructure; to provide response to cyber incidents in the field of national security [Law of Ukraine "On Basics of Providing Cyber Security of Ukraine" 2017].

The unit of the SSU responsible for conducting these functions is the Cyber Security Department, whose official name is the Department of Counterintelligence Protection of State Interests in the Sphere of Information Security. This counterintelligence body is the main actor of the National Cyber Security System which protects national security of Ukraine from cyber threats. At present, it concentrates mostly on countering Russian cyber operations organized by Russian special services.

Within the framework of the NATO Trust Fund on Cyber Defense for Ukraine the Situational Center for Cybersecurity of the Security Service of Ukraine was created in 2017 [Security Service of Ukraine. *Holova SBU vidkryv Sytuatsiynyy tsentr zabezpechennya kibernetychnoyi bezpeky*]. This is a unique structure as it combines functions and technical abilities of CERT/CSIRT with counterintelligence tools and instruments of special service and law enforcement bodies.

It already proved to be very effective in countering cyber threats of hybrid warfare and greatly facilitated the capacities of the Security Service of Ukraine in Cyber Security. During 2018–2019, three regional Cyber Security Centers of the SSU have been established in the cities of Dnipro, Odessa and Sumy. Their main task is to counter cyber threats at the regional level. Another important direction of developing the SSU capabilities is promotion of public-private partnership, impossible to counter cyber threats effectively without cooperation with the private sector. Firstly, because more than 80% of Ukrainian critical infrastructure is privately

owned and secondly, the nature of cyber threats and cyber space makes no difference between the character of threats to the public sector or to national security.

Professionals of the Cyber Security Situational Awareness Center of the SSU on the basis of the NATO standards created the Malware Information Sharing Platform – Ukrainian Advantage (MISP-UA). This platform provides on-line automatic information exchange between Security Service of Ukraine and Critical Infrastructure about indicators of compromise and possible cyber threats. The MISP-UA is not yet being used for international information exchange but it might be considered as a further step for its development. Through this platform, the SSU provides the private sector with timely information which is important to protect their computer systems from cyberattacks and greatly contributes to enhancing the security of critical infrastructure. At present, there are more than 30 Critical Infrastructure Facilities in the sphere of energy, telecommunications, transport, or finance connected to the MISP-UA. The legal basis for such cooperation is the Memorandum for Information Sharing [Security Service of Ukraine. *SBU posylyuye zakhyst informatsiynoyi bezpeky pidpryyemstv enerhetychnoyi haluzi Ukrayiny*].

The National Police of Ukraine ensures the protection of human and civil rights and freedoms, the interests of society and the state from criminal encroachments in cyberspace. It carries out measures on prevention, detection, suppression and disclosure of cybercrime, raising awareness of citizens about security in cyberspace. The direct execution of these tasks is entrusted to the Department of Cyber Police of the National Police of Ukraine, established on October 13, 2015, which replaced the Office for Combating Cybercrime of the Ministry of Internal Affairs of Ukraine [Decree of the Cabinet of Ministers of Ukraine No. 831 of 13 October 2015].

The Department of Cyber Police consists of structural divisions, acting on the interregional basis and directly subordinated to the Head of the Department. In accordance with the Law of Ukraine "On Ratification of the Convention on Cybercrime" [2005], in order to ensure the international cooperation of Ukraine on combating cybercrime, the National 24/7 point of contact for the immediate assistance in investigation of cybercrimes is functioning in the structure of the Department of Cyber Police.

The Ministry of Defense and the General Staff of the Armed Forces of Ukraine – among the main tasks of these authorities there are: carrying out measures to prepare the state for reflecting military aggression in cyberspace (cyber defense); carrying out military cooperation with NATO and other defense actors in the field of security of cyberspace and joint protection against cyber threats; implementing measures to ensure cyber defense of critical information infrastructure in conditions of emergency and martial law.

The National Cybersecurity Coordination Center (NCCC), as the working body of the National Security and Defense Council of Ukraine, coordinates and monitors the activities of the security and defense sector providing cybersecurity; forecasts and identifies potential and actual cyber threats, generalizes international experience in the field of cyber security; provides operational, informational and

analytical support of the National Security and Defense Council of Ukraine on cybersecurity issues.

The NCCC was created in June 2016 by the Decree of the President of Ukraine No. 242/2016 and according to the former Secretary of the National Security and Defense Council of Ukraine Mr. Turchinov, it were to become a system-forming element of the whole system of cyber security and cyber defense of Ukraine [National Security and Defense Council of Ukraine. *O. Turchynov: Natsional'nyy koordynatsiynyy...* 2016]. The Head of the Center is the Secretary of the National Security and Defense Council of Ukraine. The Secretary of the Center is the Head of the structural unit of the apparatus of the National Security and Defense Council of Ukraine, whose responsibilities include cybersecurity.

THE MAIN CHALLENGES OF UKRAINE'S CYBERSECURITY SYSTEM FURTHER DEVELOPMENT

Ineffective Cybersecurity Strategy Implementation – though Ukraine has made a substantial step forward in the cyber security domain, the main obstacle that hampers its further development is the lack of the effective mechanisms of implementing cybersecurity policies, in particular the provisions of the Cybersecurity Strategy of Ukraine and the formal approach to this issue by responsible state authorities.

Many other important issues have still not been resolved:

- the Register of Critical Infrastructure Information Systems as well as the legal framework for its protection is not created,
- the Budapest Convention on Cybercrime is not fully implemented,
- the secure data center for governmental bodies is not built,
- any effective measures to stimulate the development of domestic software are not being taken,
- the EU directives and standards for the protection of critical infrastructure are not implemented,
- no system of cyber security auditing of such objects or main indicators of cybersecurity and risk assessment are formed,
- a unified system of cyber threats detection and information exchange between the main state actors of cyber security is not created,
- many gaps in cyber security legislation are still not closed, etc.

Other efforts should be directed at building a legal framework for critical information infrastructure protection by adopting the National Register of Critical Information Objects and a framework law establishing the main requirements and responsibilities of their owners in the sphere of cyber protection. Furthermore, providing a high level of critical infrastructure resilience is impossible without updating domestic standards of cyber security on the basis of international and European standards in this sphere.

CONCLUSIONS

In the article we have shown that both systems of national cyber security have their own advantages, however, there are still vast bottlenecks, such as inconsistency in terms of inter-agency cooperation, lack of information sharing, and subsequently – lack of synergistic effect from the interagency cooperation.

Polish doctrinal approach makes a distinction between the nature, objectives, and methods of many internal and external threats, claiming that national cybersecurity is affected by the actors operating in cyberspace with various skills, targets, and motivations, emphasizing that the number of states capable of and actually initiating cyberattacks is increasing. External threats listed by the doctrine include cyber crises, cyber conflicts, cyberwar, and cyberespionage involving states and other entities, "threats (for Poland) coming from cyberspace include extremist, terrorist and international criminal organizations whose attacks in cyberspace can have ideological, political, religious, business or criminal motivations" [*Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej* 2015]. The current model of strategic and institutional coordination of the cybersecurity system of the Republic of Poland is criticized, but its prompt response to cyber incidents is considered to be quite effective. Poland has a multi-layered approach to cyberattacks. This can be seen in the quick evaluation of risks the national security, or the harmonized division of the tasks between the state institutions that deal with preventing cyberattacks both at the national and regional level. This comprehensive approach to cyberattacks is reflected in Poland's cybersecurity strategy.

Meanwhile, in case of Ukraine, efforts should be directed at building a legal framework for critical information infrastructure protection by adopting the National Register of Critical Information Objects and a framework establishing the main requirements and responsibilities of their owners. What remains true for both countries is the logic that providing a high level of critical infrastructure resilience is impossible without updating domestic standards of cyber security on the basis of international and European standards in this sphere.

In the face of the widespread globalisation processes and the related informational interdependence between countries, cross-border cooperation is crucial for achieving security in global informational and cyberspace. While carrying out these tasks at the European level, it is important for Poland to intensify its efforts to ensure the security of the Digital Single Market but also to involve countries outside of the EU in this process as a part of the approximation to the Digital Single Market. It would also be important in further development of the Common Foreign and Security Policy of the European Union.

In addition to reinforcing its international position, Poland will benefit from collaboration with corresponding institutions and agencies responsible for ensuring cybersecurity in Ukraine. Cooperation at the operational and technical level could be carried out, *inter alia*, via the CSIRT Network at the European Union level, through other international cooperation networks, like the FIRST

or TF-CSIRT, or through information sharing platforms of different kinds, etc. Therefore, Ukraine still needs to implement proper mechanisms. Thus, it would be important to develop common operational procedures between the two countries. Since the operational frameworks of governmental structures responsible for ensuring cybersecurity in Poland and in Ukraine are structurally similar, it gives an additional opportunity to fine-tune both systems as far as tackling cross-border incidents is concerned, as in the case of EMOTET malware takedown that was a joint effort of EU and Ukrainian cyber infrastructure systems [https://twitter.com/i/status/1354407402020466689].

Tytuł: Porównanie systemów cyberbezpieczeństwa Polski i Ukrainy

Streszczenie: Zapewnienie bezpieczeństwa informacji będące wyzwaniem w nowej rzeczywistości związanej z COVID-19 jest niezbędne do jego rozszerzenia poza granice kraju, przez krajowe systemy cyberbezpieczeństwa, na podmioty tworzące krajowy system cyberbezpieczeństwa, czyli podmioty gospodarcze świadczące usługi z wykorzystaniem systemów teleinformatycznych użytkowników, władze publiczne oraz wyspecjalizowane podmioty zajmujące się bezpieczeństwem teleinformatycznym na poziomie operacyjnym w różnych krajach.
Jak podkreśla wielu badaczy, wszelkie znaczące zakłócenia w funkcjonowaniu informacji i cyberprzestrzeni, zarówno globalne, jak i lokalne, mają wpływ na bezpieczeństwo transgraniczne, wydajność instytucji sektora publicznego, procesy produkcyjne i usługowe oraz ostatecznie na bezpieczeństwo narodowe, wspólnotowe, ale także osobiste [Anderson, Hern 1996; Buzan, Wæver, de Wilde 1998; Deibert 2002; Hansen, Nissenbaum 2009; Świątkowska 2012].
Celem artykułu jest bliższe przyjrzenie się ramom działania struktur rządowych odpowiedzialnych za zapewnienie cyberbezpieczeństwa w Polsce i na Ukrainie. Przykład Polski jest ważny, ponieważ jest ściśle powiązany z ramami cyberbezpieczeństwa NATO, UE, ONZ i OBWE. Współpraca ta odgrywa ważną rolę w walce z rosnącą liczbą incydentów. Tymczasem Ukraina przygotowuje się do członkostwa w ogólnoeuropejskich i transatlantyckich sieciach informacji i cyberbezpieczeństwa, czyli ważne jest, aby dobrze rozumieć system cyberbezpieczeństwa i jego wąskie gardła.

Słowa kluczowe: cyberbezpieczeństwo, polityka bezpieczeństwa informacji, ENISA, ramy polityki cyberbezpieczeństwa

REFERENCES

1. Anderson R.H., Hearn A.C. (1996), *An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: "The Day After … in Cyberspace II"*, Santa Monica.
2. Buzan B., Wæver O., de Wilde J. (1998), *Security – a New Framework for Analysis*, London.
3. *CERT-UA: skoraya kiberpomosht'* (*CERT-UA: Cybersecurity Emergency*). (2014), "PCWeek/UE", No. 4, https://www.pcweek.ua/themes/detail.php?ID=147850 [access: 18.10.2020].
4. Cyber Security Department, https://www.gov.pl/web/digitalization/cyber-security-department [access: 22.04.2021].
5. Decree of the Cabinet of Ministers of Ukraine No. 831 of 13 October 2015, https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF [access: 18.10.2020].

6. Decree of the President of Ukraine of 27 January 2016 On the Decision of the National Security and Defense Council of Ukraine "On the Cyber Security Strategy of Ukraine", https://zakon5.rada.gov.ua/laws/show/96/2016 [access: 18.10.2020].
7. Deibert R. (2002), *Circuits of Power: Security in the Internet Environment*, [in:] *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, eds. J.N. Rosenau, J.P. Singh. Albany.
8. Departament Cyberbezpieczeństwa przy Ministerstwie Cyfryzacji (Department of Cybersecurity at the Ministry of Digitalization), https://www.gov.pl/web/cyfryzacja/departament-cyberbezpieczenstwa [access: 17.10.2020].
9. Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0590 [access: 17.10.2020].
10. *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*. (2015), https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf [access: 18.04.2021].
11. Emergency Response Team of Ukraine. *Skorystaytesya nashoyu dopomohoyu v likvidatsiyi kiberzahroz* (*Use Our Help to Liquidate Cyber Threats*), https://cert.gov.ua/ [access: 18.10.2020].
12. Emergency Response Team of Ukraine. *Vidkryttya Tsentru reahuvannya na kiberzahrozy* (*Opening of Cyber Threat Response Center*), https://cert.gov.ua/news/25 [access: 18.10.2020].
13. Hansen L., Nissenbaum H. (2009), *Digital Disaster, Cyber Security, and the Copenhagen School*, "International Studies Quarterly", Vol. 5(3). DOI: https://doi.org/10.1111/j.1468-2478.2009.00572.x.
14. https://twitter.com/i/status/1354407402020466689 [access: 17.04.2021].
15. Law of Ukraine "On Basics of Providing Cyber Security of Ukraine". (2017), https://zakon.rada.gov.ua/laws/show/2163-19 [access: 18.10.2020].
16. Law of Ukraine "On the Ratification of the Convention on Cybercrime". (2005), https://zakon.rada.gov.ua/laws/show/2824-15 [access: 18.10.2020].
17. Ministerstwo Cyfryzacji, https://www.gov.pl/web/cyfryzacja [access: 17.10.2020].
18. National Security and Defense Council of Ukraine. (2016), *O.Turchynov: Natsional'nyy koordynatsiynyy tsentr kiberbezpeky povynen mobilizuvaty ves' nayavnyy potentsial dlya zabezpechennya nadiynoho kiberzakhystu krayiny* (*O. Turchinov: National Cybersecurity Coordination Center Should Mobilize All Capacities for Cyber Protection of State*), https://www.rnbo.gov.ua/ua/Diialnist/2528.html?PRINT [access: 18.10.2020].
19. Naukowa i Akademicka Sieć Komputerowa (Scientific and Academic Computer Network), https://www.nask.pl/ [access: 17.10.2020].
20. Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa. (2020), (Amendment to the act on the national cybersecurity system), https://www.cyberdefence24.pl/nowelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-odpowiedz-na-wyzwania-wspolczesnego-swiata [access: 17.10.2020].
21. Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 16 maja 2019 r. w sprawie ogłoszenia jednolitego tekstu ustawy – Kodeks pracy, Dz.U. 2019 poz. 1040 (Announcement of the Marshal of the Sejm of the Republic of Poland of 16 May 2019 on the publication of the consolidated text of the Act – Labor Code, Journal of Laws of 2019 item 1040), http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190001040 [access: 17.10.2020].
22. Park D., Walstrom M. (2017), *Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks*, https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/ [access: 18.10.2020].

23. *Powstaje Kolegium ds. Cyberbezpieczeństwa* (*On the College of Cybersecurity*), https://www.gov.pl/web/cyfryzacja/powstaje-kolegium-ds-cyberbezpieczenstwa [access: 17.10.2020].
24. Rada do Spraw Cyfryzacji, https://www.gov.pl/web/cyfryzacja/rada=-do-spraw-cyfryzacji?fbclid=IwAR3jBCf9Lonk3YkJrzCQcGRDpwkJ3r2YuMU8IfdVO05HrcFenJ7HnmzsOAw [access: 17.10.2020].
25. Rozporządzenie Rady Ministrów z dnia 2 października 2018 r. w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa (Ordinance of the Council of Ministers of 2 October 2018 on the scope of activities and working procedures of the College for Cybersecurity), https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/zakres-dzialania-oraz-tryb-pracy-kolegium-do-spraw-cyberbezpieczenstwa-18764810 [access: 17.10.2020].
26. Security Service of Ukraine. *Holova SBU vidkryv Sytuatsiynyy tsentr zabezpechennya kiberne-tychnoyi bezpeky* (*Head of SSU Opens Cyber Security Situational Awareness Center*), https://ssu.gov.ua/ua/news/1/category/21/view/4318#.7sucy46n.dpbs [access: 18.10.2020].
27. Security Service of Ukraine. *SBU posylyuye zakhyst informatsiynoyi bezpeky pidpryyemstv enerhetychnoyi haluzi Ukrayiny* (*SSU Strengthens Protection of Information Security of Ukraine's Energy Sector*), https://ssu.gov.ua/ua/news/1/category/21/view/5213#.ARNTdGPL.dpbs [access: 18.10.2020].
28. Świątkowska J. (2012), *Zagrożenia cyberprzestrzeni wyzwaniem dla bezpieczeństwa współczesnego świata*, [in:] *Współpraca państw Grupy Wyszehradzkiej w zapewnieniu cyberbezpieczeństwa – analiza i rekomendacje*, red. J. Świątkowska, Kraków.
29. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2005 Nr 64 poz. 565 (Act of 17 February 2005 on computerization of the activities of entities performing public tasks, Journal of Laws of 2005 No. 64 item 565), http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20050640565/U/D20050565Lj.pdf [access: 17.10.2020].
30. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560 (Act of 5 July 2018 on the national cybersecurity system, Journal of Laws of 2018 item 1560), https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560&fbclid=IwAR22MHvcWrXmiPm-7YFy_Je7zS2OeNql6dMuOZxTIYCarcW4u4Oi2lw8MmU [access: 17.10.2020].
31. Ustawa z dnia 19 lipca 2019 r. o zmianie ustawy o minimalnym wynagrodzeniu za pracę, Dz.U. 2018 r. poz. 2177 i 2019 r. poz. 1564 (Act of 19 July 2019 on the on the amendment to the act on the minimum remuneration for work, Journal of Laws of 2018 item 2177 and of 2019 item 1564), http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20190001564/T/D20191564L.pdf [access: 17.10.2020].