Cooperation Mechanisms to Ensure the Security of Network and Information Systems in the Light of the NIS Directive

MONIKA NOWIKOWSKA

Abstract In recent years we have seen a spike in interest in cybersecurity, resulting in an increasing number of individuals and organisations being established to deal with this problem. However, in order to carry out public tasks in this area more effectively, it is necessary for particular entities to cooperate and exchange information. Cooperation mechanisms to ensure the security of network and information systems are defined in Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high, common level of security of network and information systems across the Union (OJ EU L 194/1).

Keywords: • network and information systems • cyberspace • public administration • cooperation • single point of contact • CSIRT • Cooperation Group

CORRESPONDENCE ADDRESS: Monika Nowikowska, Ph.D., Assistant Professor, War Studies University in Warsaw, Institute of Law, Department of New Technologies and Cybersecurity Law, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warszawa, Poland, e-mail: m.nowikowska@akademia.mil.pl, ORCID: 0000-0001-5166-8375.

https://doi.org/10.4335/2022.2.6 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

In an era of the constant development of new technologies, networks, as well as information, systems and services are essential for any state to operate. Fundamental importance is attributed to the internet, which plays a primary role in facilitating the cross-border movement of goods, services and people. Due to its global, supranational character, the importance of the proper functioning of networks and systems, their reliability and security constitute a *sine qua non* condition for the efficient functioning of states and societies. The scale, frequency and impact of security incidents are becoming more and more important and pose a serious threat to the functioning of network and information systems. These systems may also become an object of intentional harmful actions aimed at damaging or disrupting their operation (Chałubińska-Jentkiewicz, Nowikowska, 2020:305).

Furthermore, public authorities have been obliged to provide citizens with electronic services covering both the handling of citizen matters and other areas of public administration operation. The processes of the computerisation of public administration are accompanied by changes related to the mode of operation in the state-citizen relationship (Chałubińska-Jentkiewicz, 2019:68). Thus, IT services have become an essential tool to ensure the efficiency of administrative apparatus (Knosala, Matan, Zacharko, 1999:126).

In order to promote and facilitate strategic cooperation between states on the security of network and information systems at the European Union level, the European Parliament and the Council of the European Union adopted on 6 July 2016 Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the so-called NIS Directive) (OJ EU L194/1). The preamble of the NIS Directive indicates that the existing capabilities are not sufficient to ensure a high level of security of network and information systems. Member States have very different levels of preparedness, which has led to fragmented approaches towards the issues related to the security of network and information systems across the Union. In consequence, this may result in an unequal level of protection of consumers and businesses, and undermines the overall level of security of network and information systems within the Union. Similarly, a lack of common requirements on the operators of essential services and digital service providers makes it impossible to set up a global and effective mechanism for cooperation between Member States. Thus, in order to respond effectively to the challenges of the security of network and information systems, a decision was made to adopt a global approach at the Union level covering i.e., common minimum capacity building and planning requirements, the exchange of information, cooperation and common security requirements for operators of essential services and digital service providers.

As a consequence of the adoption of the NIS Directive and for the purpose of establishing a coherent system to ensure cybersecurity of the Republic of Poland, on 5 July 2018 the Sejm of the Republic of Poland enacted the Act on the National Cybersecurity System, which entered into force on 28 August 2018. The said Act and the accompanying implementing regulations have fully implemented the provisions of the NIS Directive into the Polish legal order.

The subject matter of this paper are the mechanisms of cooperation to ensure the security of network and information systems in the light of the NIS Directive. This topic required an analysis of the content and evaluation of the source literature (using the *desk research* technique) and of the selected EU and Polish legal acts, covering three fundamental issues: the concept of network and information systems, the concept of cyberspace and the *ratio legis of* establishing cooperation mechanisms to ensure the security of network and information systems.

2 The concept of network and information systems

The concept of network and information systems is defined in Article 4 of the NIS Directive. According to that provision, “network and information systems” means: a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108, 24/04/2002) b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance.

Within the meaning of Article 2(a) of Directive 2002/21/EC (a) “electronic communications network” means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.

The Union legislator also chose to define the “security of network and information systems”, which means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.

It should be noted that this definition is consistent with the definition of information security contained in ISO/IEC 27001:2005 and ISO/IEC 17799:2007. The ISO/IEC 17799:2007 Guide to Information Security Management System defines information security as the preservation of information properties, i.e., *confidentiality*, *integrity*, *availability*, *accountability*, *authenticity*, *non-repudiation* and *reliability*. The first three properties - confidentiality, integrity and availability – form the backbone for building an information security system. Their importance varies from organisation to organisation. For government institutions, confidentiality is important. For organisations producing statistical research, the most important property will be integrity during data processing. These entities must not make any mistakes, as this can have a very negative impact on their credibility. Availability, on the other hand, is the most important condition for all entities in the service industry, where any short interruption in business operations can result in exponential financial loss (Łuczak, Tyburski, 2009:12). Information confidentiality, integrity, availability, accountability, authenticity, non-repudiation and reliability are the so-called attributes of information security (Chałubińska-Jentkiewicz, Nowikowska, 2020:34).

Confidentiality *means ensuring that information is only accessible to authorised persons with the appropriate right of access.* In other words, confidentiality can be construed as the ability to make information available for common use by many people, while at the same time not making it available to those who should not read it. *Maintaining confidentiality is present to prevent the detection of the source of transmission*, data *destination*, frequency, length and other transmission characteristics. Loss of confidentiality may occur during information handling, for instance while copying it. Despite various measures to ensure confidentiality, there is a risk of accidental or intentional breaches of confidentiality. Therefore, a security system should not only ensure confidentiality, but also guarantee the possibility of detecting attempts to breach confidentiality and the breaches themselves. A fundamental aspect for maintaining confidentiality is to define a closed list of persons, the so-called depositaries, who can read the information. The ability of an organisation to maintain confidentiality is essentially based on the management of classified information. Once an organisation has identified any specific information that requires confidentiality protection, it is possible to introduce rules and methods for handling the given information. This primarily concerns: the marking of information and the rules for its copying, storage, destruction, and sharing (Łuczak, Tyburski, 2009:13).

Integrity means the tracking of information processing in all its forms to prevent unauthorised modification, or to eliminate an incorrect processing method. We can speak of maintaining the integrity of information when any intentional or unintentional unauthorised modification of information is impossible. Ensuring integrity is essential when it is possible for the user to modify data in a way that may cause the information to be false, incomplete or falsified. A key aspect for maintaining integrity is access control.

This means ensuring that information is created or updated in a controlled manner and is protected against damage or destruction.

Availability, on the other hand, means the assurance that information is available to an authorised person at any time that that person may need it. The loss of availability as one of the properties of information security may lead, most often, to a loss of business continuity, and thus productivity. It may result in a loss of income, as well as generate direct or indirect financial losses. Lack of access to a specific piece of information may result in an organisation failing to complete its tasks on time. Considering the equipment that supports an information system, it should be designed in such a way so as to ensure its high availability and redundancy of all major components, including disk drives, power supplies, fans, etc., so that repairing a failed component should not cause any downtime. It is the infrastructure that modern information systems rely on. The two most important infrastructure components are power supply and telecommunications. The availability of power or the elimination of interruptions in supplying information systems with power is deemed to be a basic need. Uninterruptible power supplies and backup generators provide power in the event of an interruption. Network availability is based on redundancy in networks and multiple supplies, making the network even more accessible. In addition, it is necessary to ensure the possibility to repair and replace any part of this system without causing significant downtime of equipment in contact with information. This will guarantee optimum performance and minimum impact due to any damage. A system that remains available should be equipped with a real-time backup function. Such a solution will enable access to the latest data, even in the case of any unintentional loss of information by an employee. Availability in organisations hinges primarily on the ability to avoid or overcome the factors that cause downtime, or on the ability to quickly remove downtime (Łuczak, Tyburski, 2009:15).

Therefore, the basic components of information security are: information security management, network security, policy, data and computer security (Chalubinska-Jentkiewicz, Nowikowska, 2020:36).

Under Polish law, the terminology relating to the network and information system notions analysed herein is not uniform, which causes a number of controversies. Particular normative acts use different concepts, such as: information systems (*systemy informacyjne),* IT systems *(systemy informatyczne)*, and communication and information systems (*systemy teleinformatyczne*), which may be mistakenly treated as synonyms. In 2016, the term “information system” appeared in 390 acts published in the Journal of Laws, “IT system” – in 1242 and “communication and information system” – in 1138 (Szpor, 2016:120). In order to discuss the issue of cooperation mechanisms to ensure security in cyberspace, it seems necessary to put the terminology discussed herein in order.

Information systems is a legal term that appeared in the 1990's, among others in the Act of 29 June 1995 on Official Statistics (Journal of Laws of 2021, item 955). The notion of public administration information systems covers systems for collecting, gathering and processing information by public administration bodies, the Social Insurance Institution (ZUS), the National Health Fund, the Financial Supervision Authority (KNF), registration bodies, other legal bodies of the state or local government, as well as other entities keeping official registers (Article 2(13)).

IT system is defined, among others, in the Act of 24 August 2007 on the Participation of the Republic of Poland in the Schengen Information System and the Visa Information System (Journal of Laws of 2021, item 1041).”IT system” is construed as a set of cooperating devices, information processing procedures and SW tools (software) used for data processing, along with the telecommunication infrastructure enabling public administration bodies and justice administration bodies to process the data collected in the Schengen Information System and the Visa Information System.

In the source literature an IT system is construed as a device or a group of interconnected or related devices (i.e., hardware), such as a processor or a central processing unit together with the peripheral devices connected thereto (monitor, printer, etc.), if any, as well as the software enabling automatic data processing. Hence, it will be a mobile phone or a personal computer (Radoniewicz, 2019:46).

Communication and information system is a term that appears, among others, in the regulation on the protection of classified information. A communication and information system is defined in Article 2(6) of the Act of 5 August 2010 on the Protection of Classified Information (Journal of Laws of 2019, item 1228). “Communication and information system” shall be construed as defined in Article 2(3) of the Act of 18 July 2002 on the Provision of Services by Electronic Means (Journal of Laws of 2020, item 344). Since the legislator made reference to another act, a communication and information system on the grounds of protection of classified information means a set of cooperating IT devices and software, ensuring processing and storing, as well as sending and receiving data through telecommunications networks by means of terminal equipment appropriate for the given type of network, within the meaning of the Act of 16 July 2004 – Telecommunications Law (Journal of Laws of 2021, 576). The source literature indicates that a photocopier is a communication and information system – within the meaning of the Act of 5 August 2010 on the Protection of Classified Information – which makes it possible to prepare and store classified information on a computer data carrier (Anzel, 2018:73). It seems that the term “communication and information system” emphasises the connection with telecommunications, which is currently defined by law as the emission, reception or transmission of information, irrespective of its type, by wire, radio, optical or other electromagnetic means.

On the other hand, telecommunications network, according to Article 2(35) of the Telecommunications Law, means transmission systems and switching or routing equipment as well as other resources, including non-active network elements, which enable the emission, reception or transmission of signals by wire, radio, optical or other electromagnetic means, irrespective of their type; (Krupa, 2020:183).

To summarise the above, it should be stated that an interdisciplinary agreement on the relations between the concepts of "communication and information system", "IT system" and "information system" is desirable. Under the NIS Directive, the legislator used the term *information system,* which was translated into Polish as *systemy informatyczne* (IT systems). In view of the fact that the term "information systems" is often used in the Polish legal language, where the term is generally construed as cooperating devices, information processing procedures and SW (software) tools used for the purpose of data processing, and the telecommunications infrastructure enabling the processing of collected data, using this very term seems appropriate. It includes both technical infrastructure and information resources (*content).* The term "IT systems" used in the Polish version of the Directive may lead to a narrowing of the meaning of this concept to hardware and software, marginalising the importance of security of the content processed in IT systems.

3 Concept of cyberspace

Under both Union law and Polish legislation, there is no single legal definition of cyberspace. It is an underspecified concept. There is also no universally accepted definition of cyberspace. The term *cyberspace* originates from the combination of two words: *cybernetics* and *space,* which means cybernetic space. The term emerged in the 1980's. It is believed to have been coined by the Canadian writer W. Gibson in his 1984 novel "Neuromancer" to describe the computer-generated virtual reality in which his protagonists found themselves. The term has permeated into mass culture and is now used primarily to describe virtual space, i.e. the space of communication via computer networks (Radoniewicz, 2019:33).

In Polish law the term appears in various acts which give an autonomous meaning to the term "cyberspace". For example, in Article 2(1a) of the Act of 18 April 2002 on the State of Natural Disaster (Journal of Laws of 2017, item 1897), cyberspace is construed as the space for the processing and exchange of information created by communication and information systems, as defined in Article 3(3) of the Act of 17 February 2005 on the Computerisation of the Operations of the Entities Performing Public Tasks (Journal of Laws of 2021, item 670), together with their mutual interrelations and interactions with users. A communication and information system, within the meaning of the Act on the Computerisation of the Operations of the Entities Performing Public Tasks, is a set of IT devices and software, ensuring processing and storing, as well as sending and receiving data through telecommunications networks by means of terminal equipment appropriate for the given type of network (Czarnecka, 2019:67). The term “cyberspace” understood in this way has also been repeated in the Act of 29 August 2002 on the Martial Law and the Competences of the Commander-in-Chief of the Army and the Rules of Commander-in-Chief's Subordination to the Constitutional Authorities of the Republic of Poland in Article 2(1b) thereof (Journal of Laws of 2017, item 1932) and the Act of 21 June 2002 on the State of Emergency in Article 2(1a) thereof (Journal of Laws of 2017, item 1928). Thus, as it stems from this relatively broad definition, the legislator construes cyberspace not only as communication and information systems, i.e. the devices (hardware) they consist of, together with the programs (software) ensuring the performance of functions by these systems (processing, storage and transmission of computer data), but also as computer data (information) and interactions between devices and their users (see more broadly Aleksandrowicz, Liedel, 2012:23; Liderman, 2017:62-63).

To sum up the foregoing, it can be stated that in accordance with the definition of cyberspace adopted under the acts on extraordinary states it contains both the term “information” and the term “communication and information systems”, which terms are the core of the definition of cyberspace. Given the use of the expressions "mutual interrelations" (relations between communication and information systems) and "relations with users", which are not catalogued by the legislator, one may try to argue the definition of cyberspace is a type of definition whose scope is incomplete. By design, incomplete definitions do not list all elements of the scope, but limit themselves only to highlighting an example of these elements (Taczkowska-Olszewska, 2019:4). However, this observation may also lead to the opposite thesis, according to which a rational legislator did not concretise the types and features of the said relations existing between subjects (users) of cyberspace, intending to achieve the goal of covering all types of activity with this term, regardless of the status of any subjects, time, place or purpose of undertaking it, with the reservation that this activity takes place with the use of communication and information systems, and its object is information (Taczkowska-Olszewska, 2017:53).

In the source literature, M. Lakomy emphasises that cyberspace is a global information infrastructure, the interconnectivity between people by means of computers and telecommunications (Lakomy, 2015:67). Similarly, P. Levy notes that cyberspace is an information domain, a space for open communication through computers around the world (Levy, 2002:380).

The analysis of doctrinal definitions of cyberspace allows us to identify certain elements characteristic of the cyberspace environment. They include: 1) unlimited reach; 2) the welding of information resources into huge databases; 3) no possibility to reference cyberspace to the physical dimensions of the real world (Wasilewski, 2013:226), 4) the complexity of the phenomenon, by basing cyberspace on technical, technological and social elements (Dobrzeniecki, 2004:21), 5) the combination of communication and information systems, information and interactions between devices and their users (Radoniewicz, 2019:49).

The need to take action to determine the standard norms, principles and values in cyberspace was indicated by the European Commission in its Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions entitled "Cybersecurity Strategy of the European Union: an open, safe and secure cyberspace" (EU Commission Communication of 7.2.2013, JOIN(2013), 1 final) – hereinafter the Communication. In this Communication, the Commission stressed that fundamental rights, democracy and the rule of law need to be protected in cyberspace. Freedom in the online environment requires safety and security. Cyberspace should be protected from incidents, malicious activities and misuse; and governments have a significant role in ensuring a free and safe cyberspace, whose mission should be to respect and protect fundamental rights online and to maintain the reliability and interoperability of the internet. However, the private sector owns and operates significant parts of cyberspace, and so any initiative in this area has to recognise its leading role (Chalubinska-Jentkiewicz, Nowikowska, 2020:21).

One of the key regulatory objectives is to ensure cybersecurity, which requires actions related to maintaining the availability and integrity of networks and infrastructure, as well as the confidentiality of any information contained therein, subject to the right of privacy and with respect for identity. Ensuring cybersecurity becomes one of the fundamental objectives of the State, and the determinant of these principles is the protection of fundamental values, which should have the same degree of protection in cyberspace as in the real world. Cyberspace that is open and free removes social and international barriers, allows the exchange of cultures and experiences between states, communities and individuals, enabling interactions and the exchange of information, and consequently the exchange of knowledge, experience and technology.

The way in which cyberspace is defined, as well as the place in a system of legal acts in which this definition is placed, determine both the need for inseparable protection of the content of information and the methods of its transmission, recording, generation and storage, as well as – on the other hand – the rank of information in the hierarchy of legally protected interests. The rank of information has increased. Not only because in the era of an information society it has become a factor of the economic growth of states, but mainly down to the value of information as a new kind of weapon and a tool of war used in a new arena of the fifth theatre of war, besides land, air, water and space, which cyberspace has become (Chalubinska-Jentkiewicz, Karpiuk, 2015:57; Liedel, 2011:48; Lakomy, 2015:63). It is de facto synonymous with “information space” construed as aggregated information resources available to an individual with the use of communication and information systems. Therefore, cyberspace can be seen as "the space of information created by all computer networks put together" (Denning, 2002:25).

4 Cooperation mechanisms

In order to respond effectively to the challenges of ensuring the security of network and information systems in cyberspace, the EU legislator has indicated the need to build a common, comprehensive approach, covering, among others, the exchange of information and cooperation between Member States.

An analysis of the provisions of the NIS Directive makes it possible to distinguish cooperation mechanisms at two levels: 1) a technical level and 2) a political and strategic level.

Cooperation in technical terms is to be ensured through a European CISRT network and the creation of mechanisms for the exchange of information on cross-border incidents between CSIRTs designated for operators of essential services and digital service providers.

Cooperation in the political and strategic dimension is to be implemented through the establishment of a Cooperation Group, which will develop joint strategic conceptions and receive, inter alia, annual reports from competent authorities.

The Directive did not determine the precise mechanisms of operation in the two fora. Both the CSIRT Network and the Cooperation Group are to define them themselves.

In order to be able to cooperate effectively with economic actors, Member State bodies need to be structured accordingly. Hence, the NIS Directive distinguishes between points of contact and the computer security incident response teams (called “CSIRTs”). The single points of contact should not directly receive any notifications of incidents. This task belongs to the CSIRTs. The designated point of contact is however required to forward incident notifications to the single points of contact of other affected Member States. To ensure the effective provision of information to the Member States and to the Commission, a summary report should be submitted by the single point of contact to the Cooperation Group, and should be anonymised in order to preserve the confidentiality of the notifications and the identity of operators of essential services and digital service providers, as information on the identity of the notifying entities is not required for the exchange of best practice in the Cooperation Group. The summary report should include information on the number of notifications received, as well as an indication of the nature of the notified incidents, such as the types of security breaches, their seriousness or their duration.

Recital 31 of the NIS Directive stipulates that in order to facilitate cross-border cooperation and communication, it is necessary for each Member State to designate a national single point of contact responsible for coordinating issues related to the security of network and information systems and cross-border cooperation at the Union level.

Competent authorities and single points of contact should have the adequate technical, financial and human resources to ensure that they can carry out the tasks assigned to them in an effective and efficient manner and thus achieve the objectives of this Directive.

The Single Point of Contact serves communication within the European Union. The exchange of information between EU Member States serves the implementation of objectives of the NIS Directive in terms of achieving a high common level of security of network and information systems in the Union. Under the Polish Act on the National Cybersecurity System, the Single Point of Contact shall forward, at the request of the competent CSIRT MON, CSIRT NASK or CSIRT GOV, notifications of a serious or significant incident concerning two or more EU Member States to the Single Points of Contact in other EU Member States. It is also required to receive notifications of a serious incident concerning two or more European Union Member States from the Single Points of Contact in other European Union Member States and then forward these notifications to the CSIRT MON, CSIRT NASK, CSIRT GOV or sectoral cybersecurity teams (Chalubinska-Jentkiewicz, 2019:296).

When implementing the NIS Directive, the Polish legislator assumed that the Minister for Computerisation, acting as the Single Point of Contact, is responsible for receiving and forwarding, at the request of relevant CSIRTs, notifications of a serious or significant incident concerning two or more Member States of the European Union. Moreover, it is responsible for ensuring the representation of the Republic of Poland in the Cooperation Group, the exchange of information for the benefit of public authorities, competent authorities in Poland and abroad, CSIRT and the fulfilment of reporting obligations towards the Cooperation Group and the European Commission.

The main tasks of the point of contact include: 1) receiving reports of a serious or significant incident concerning two or more Member States of the European Union from single points of contact in other Member States of the European Union, as well as forwarding these notifications to the CSIRT MON, CSIRT NASK, CSIRT GOV or sectoral cybersecurity teams - i.e. acquiring and forwarding information on any existing emergency situation from other points of contact in the EU, if the situation there is of a broader character, because it concerns more than one state; 2) forwarding, at the request of the competent CSIRT MON, CSIRT NASK or CSIRT GOV, notifications of a serious or significant incident concerning two or more Member States of the European Union to single contact points in other Member States of the European Union - i.e. acquiring and forwarding information about such incidents to other points of contact, which are affected by the incident 3) ensuring representation of the Republic of Poland in the Cooperation Group - i.e. fulfilling a representative function; 4) ensuring cooperation with the European Commission in the area of cybersecurity - i.e. fulfilling the policy of cooperation with the EU in the area of cybersecurity 5) coordinating cooperation between the competent authorities for cybersecurity and public authorities in the Republic of Poland with the relevant authorities in the European Union member states - i.e. coordinating the cooperation between the state and other EU states on cybersecurity; 6) ensuring the exchange of information for the needs of the Cooperation Group and the CSIRT Network - i.e. implementing information aspects of cooperation (Chalubinska, 2019:296-297).

Cooperation in the political and strategic dimension is implemented through the establishment of the Cooperation Group. The Cooperation Group - as an auxiliary tool for assessing national strategies for the security of network and information systems - should serve as a tool for exchanging best practices, discussing capabilities and preparedness of the Member States. The tasks of the Cooperation Group also include assisting the Member States in evaluating national strategies on the security of network and information systems, building capacity and evaluating exercises relating to the security of network and information systems. Furthermore, in order to promote advanced security of network and information systems, the Cooperation Group should, where appropriate, cooperate with relevant Union institutions, bodies, offices and agencies, to exchange know-how and best practices, and to provide advice on security aspects of network and information systems that might have an impact on their work, while respecting existing arrangements for the exchange of restricted information. In cooperating with law enforcement authorities regarding the security aspects of network and information systems that might have an impact on their work, the Cooperation Group should respect existing channels of information and established networks (Chalubinska-Jentkiewicz, 2019:298). In order to carry out the tasks of the Cooperation Group, the single points of contact must provide it with specific information. This is because a key element in activities related to ensuring cybersecurity is information policy.

Also noteworthy is the cooperation of the Polish Armed Forces with international bodies in the area of cybersecurity, as regulated in the Act on the National Cybersecurity System. The task defining the order of cooperation of the Armed Forces of the Republic of Poland with the relevant bodies of the North Atlantic Treaty Organisation, the European Union and international organisations in the area of national defence in the field of cybersecurity definitely requires the Minister of National Defence to look for the legal norms clearly indicated in universally binding regulations which provide for competence of this body to implement such a generally outlined task. In Article 51 of the Act on the National Cybersecurity System, the legislator indicated that the cooperation of the Armed Forces of the Republic of Poland with the relevant bodies of the North Atlantic Treaty Organisation, the European Union and international organisations in the area of national defence in the field of cybersecurity is the responsibility of the Minister of National Defence.

5 Summary

The purpose of providing information about CSIRT tasks, including the main elements of incident handling procedures, is to build a common and uniform cybersecurity system. Cooperation is widely defined as performing certain activities together with someone.

Simultaneously, the essence of relationships between individuals, defined as cooperation, is striving for a common goal or helping each other to achieve divergent goals. Cooperation means positive collaboration aimed at the achievement of the effect of synergy.

Under the NIS Directive, a system of the so-called points of contact has been designed to implement cooperation in cyberspace. Pursuant to Article 8(3) of the NIS Directive, each Member State shall designate a national single point of contact on the security of network and information systems. In Polish conditions, such a body is the Minister for Computerisation. Pursuant to Article 8(4) of the NIS Directive, the single point of contact shall exercise a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the Cooperation Group and the CSIRTs network. At the same time, under Article 11 of the NIS Directive, the Union legislator has indicated the need to establish a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States, and to achieve a high, common level of security of network and information systems in the Union. Thus, based on an analysis of the provisions of the NIS Directive one may distinguish the cooperation to ensure the security of network and information systems on two levels: a technical level, through the establishment of the CISRT and mechanisms for the exchange of information on cross-border incidents, and a political and strategic level, realised through the establishment of the Cooperation Group.

References:

Aleksandrowicz, T.R. & Liedel, K. (2012) *Analiza informacji. Teoria i praktyka* (Warsaw: Difin Publishing House).

Anzel, M. (2018) Urządzenia teleinformatyczne a sporządzanie i przechowywanie informacji niejawnych, *Informacja w Administracji Publicznej*, (3), p. 73.

Banasiński, C. (2018) Podstawowe pojęcie i podstawy prawne bezpieczeństwa w cyberprzestrzeni, In: Banasiński, C. (ed.) *Cyberbezpieczeństwo* (Warsaw: Wolters Kluwer Publishing House), pp. 22-65.

Chałubińska-Jentkiewicz, K. & Karpiuk, M. (2015) *Prawo nowych technologii. Wybrane zagadnienia* (Warsaw: Wolters Kluwer Publishing House).

Chałubińska-Jentkiewicz, K. (2019) Cyberodpowiedzialność (Toruń: Wydawnictwo Adam Marszałek).

Kitler, W., Taczkowska-Olszewska, J. & Radoniewicz, F. *Ustawa o krajowym systemie cyberbezpieczeństwa* (Warsaw: C.H. Beck Publishing House), pp. 48, 297-297.

Chałubińska-Jentkiewicz, K. & Nowikowska, M. (2020) *Bezpieczeństwo, tożsamość, prywatność – aspekty prawne* (Warsaw: C.H. Beck Publishing House).

Chałubińska-Jentkiewicz, K. & Nowikowska, M. (2020) *Ochrona informacji w cyberprzestrzeni* (Warsaw: Akademia Sztuki Wojennej Publishing House).

Czarnecka, A. (2019) Wybrane obowiązki operatorów usług kluczowych na gruncie ustawy o krajowym systemie cyberbezpieczeństwa, *Informacja w administracji publicznej*, (2), pp. 64-69.

Denning, D.D. (2002) *Wojna informacyjna i bezpieczeństwo informacji* (Warsaw: Wydawnictwo Naukowo Techniczne), p. 25.

Knosala, E., Matan, A. & Zacharko, L. (1996) *Zarys nauki administracji* (Katowice: Wydawnictwo Uniwersytetu Śląskiego).

Krupa, W. (2020) Kwalifikacja działalności podlegającej obowiązkowi wpisu do rejestru przedsiębiorców telekomunikacyjnych, *IUS NOVUM*, 14(4), pp. 181-204.

Lakomy, M. (2015) *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw* (Katowice: Wydawnictwo Uniwersytetu Śląskiego), p. 63.

Liderman, K. (2017) *Bezpieczeństwo informacyjne, Nowe wyzwania* (Warsaw: PWN Publishing House), pp. 62–63.

Liedel, K. (2011) *Transsektorowe obszary bezpieczeństwa narodowego* (Warsaw: Difin Publishing House), pp. 48-48.

Radoniewicz, F. (2019) Komentarz, In: Kitler, W., Taczkowska-Olszewska, J. & Radoniewicz, F. (eds.) *Ustawa o krajowym systemie cyberbezpieczeństwa* (Warsaw: C.H. Beck Publishing House), pp. 48, 297-297.

Szpor, G. (2017) *Jawność i jej ograniczenia, Tom I. Idee i pojęcia* (Warsaw: C.H. Beck Publishing House), pp. 120-124.

Taczkowska-Olszewska, J. (2017) Bezpieczeństwo informacyjne jako kategoria prawna. Ujęcie teoretyczne, In: Kitler, W. & Taczkowska-Olszewska, J. (eds.) *Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne* (Warsaw: Towarzystwo Wiedzy Obronnej Publishing House), pp. 53.

Taczkowska-Olszewska, J. (2019) Pojęcie cyberprzestrzeni, In: Taczkowska-Olszewska, J., Chałubińka-Jentkiewicz, K. & Nowikowska, M. (eds.) *Retencja, migracja i przepływy danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa* (Warsaw: C.H. Beck Publishing House), pp.3-9.