Katarzyna Chałubińska-Jentkiewicz[*]

Responsibility on the network – the diagnosis of the current state

Abstract

The article deals with the diagnosis of the current state in relation to responsibility in the flexible area of cyberspace which is itself hard to define, in the context of security, especially its transsectoral informative part; Polish statutory, strategic and program solutions are presented in the light of EU standards. The study includes a review of threats (mainly information and ICT infrastructure) and their scopes (systemic, economic, socio-cultural) and addressees obliged to preventive and eradication activities (primarily public authorities, but also other, e.g. commercial entities or representatives operating on the market of information society); it also touches on the substantive and institutional cooperation issues at the European level.

Key words: cyberspace, cybersecurity, responsibility, threats, informationsociety, informationinfrastructure, ICT infrastructure, communication, newtechnologies

[*] Dr hab. prof. nadzw. Katarzyna Chałubińska-Jentkiewicz, Instytut Prawa, Wydział Bezpieczeństwa Narodowego, Akademia Sztuki Wojennej w Warszawie, kierownik Katedry Prawa Mediów, Własności Intelektualnej i Nowych Technologii, e-mail: kasiachalubinska@gmail.com.

The dynamic civilizational changes which have been observed in recent years all over the world are the result of the rapid and dynamic development of information technologies as well as communication technologies which support them. Thus, cyberspace is a new sphere of the influence of these processes as the fifth area of defense activities. According to W. Kitler, the fields of security may have their own separateness and be related to specific sectors of the state, but there are-and there will be more and more of them-which are not industry-specific, but trans-sectoral, trans-disciplinary. These include, for example: information, cybernetics, anti-terrorism, political system, classified information security[1].

Generally speaking, security can be perceived primarily in a negative sense as a state characterized by the absence of threats, but also the absence of dangers, certainty, peace, protection against threats[2].

Security can be achieved by protecting the state's information resources against hostile activities of the enemy (disinformation and propaganda), as well as maintaining the ability for offensive, immediate actions against the perpetrators of these activities. The term 'network and information security' is defined in Regulation (EC) No. 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency as' the resistance of a network or information system to accidental events or illegal or deceptive activities affecting the availability, authenticity, integrity and confidentiality of data stored or transmitted, and related services offered or available through these networks and systems[3].

It should be emphasized that information security as only one of the elements of cybersecurity has been subject to regulations under criminal law (see – Offences against information – chapter 33 of the Penal Code[4]), provisions of the Personal Data Protection Act and the Act on the Protection of Classified Information. All social interactions have an impact on security, and the so-called "security culture" itself determines what the attitude to risk, threats and security of a given community is, and what values in this regard are

[1] Zob. Biała księga bezpieczeństwa narodowego Rzeczypospolitej Polskiej, BBN, Warszawa 2013, s. 19 (rys. 1).

[2] Pojęcie i zakres bezpieczeństwa informacyjnego państwa, ustalenia systemowe i definicyjne.

[3] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 460/2004 z dnia 10 marca 2004 r. ustanawiające Europejską Agencję do spraw Bezpieczeństwa Sieci i Informacji.

[4] Kodeks karny z dnia 6 czerwca 1997 r. (t.j. Dz.U. z 2018 r., poz. 1600 ze zm.).

considered to be significant. The basic design of the internet is based on the openness of both its infrastructure architecture and the culture of its creators and users. The simplicity and easiness of connecting various computers has allowed a huge increase in the number of users, and the open philosophy of its creation has built a huge, multi-level interactive medium[5].

Cybercrime is a relatively recent phenomenon, but it is developing rapidly. Currently, almost everyone has access to use the ICT network and its resources. Therefore, cybercrime, due to the increasingly common access to the network, may harm the interests of the state, which transfers some of its affairs to the field of the ICT network, which sometimes can even lead to undermining state's sovereignty[6].

It happens because not all users of data communication networks understand the mechanisms of the ICT network well, which leads to a kind of ignorance of their own security in cyberspace. We should remember that cyber crime includes both acts that reflect crime in the real world and completely new phenomena that are unique to cyberspace[7] and pose threats to the individual or the state. The main report on threats to national security identifies about 50 types of threats, with 18 of them included in the National Crisis Management Plan, the threat of cyber terrorism among them[8]. In the case of cyber attacks, only the possible effects of cyber attacks on people and property are mentioned and they include potential consequences for the population which are: threat to human life and health caused by disruptions of energy systems, traffic control, etc., loss of trust in public institutions, inability to perform professional tasks, inability to communicate.

As the potential consequences of cyber attacks in regard to properties one mentions the following: significant financial and economic losses as well as social effects, disruptions in the supply of energy, fuels, food, drinking water, and disruption to the operation of the transmission infrastructure.

In turn, crisis management covers ICT networks, but more as one of the types of transmission networks, and at the same time does not take into account the layer of sharing, processing and storing information that permeates all aspects

[5] T. Goban-Klas, *Cywilizacja medialna*, Warszawa 2005, s. 151.

[6] M. Siwicki, *Nielegalna i szkodliwa treść w Internecie. Aspekty prawno-karne*, Warszawa 2011, s. 24.

[7] K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii*, Warszawa 2015, s. 353.

[8] Online <http://rcb.gov.pl/raport-o-zagrozeniach-bezpieczenstwa-narodowego-3/>.

of the functioning of the information society. The following main categories and subcategories of threats were adopted in the report on Cyberspace Risk Assessment in Government Administration in 2013: information-oriented threats (information theft for publication or sale, information counterfeiting), threats focused on IT infrastructure (data deletion, disruption of functioning, taking over the IT systems), IT failures, insufficient competence[9].

The regulators' approach to the issue of cyberspace, cyber security and cyber responsibility results from identifying this type of protection with the need to counteract attacks directed at networks themselves, which seems unjustified, especially in the context of analyzing the concept of cyberspace[10].

The above-mentioned understanding of the notion of cyberspace entered the legal language together with the introduction of the Act of August 30, 2011 amending the Act on Martial Law and on the competences of the Supreme Commander of the Armed Forces and the rules of its subordination to the constitutional organs of the Republic of Poland and some other acts[11]. The Polish definition of the concept of cyberspace is found in the Act of 29 August 2002 on Martial Law and the powers of the Supreme Commander of the Armed Forces and the principles of its subordination to the constitutional organs of the Republic of Poland[12]. Another legal definition of the concept of cyberspace is contained in the Act of 21 June 2002 on the state of emergency[13]. According to the above Act, cyberspace is understood as "the space of processing and exchange of information created by ICT systems specified in art. 3 point 3 of the Act of 17 February 2005 on the computerization of the activities of entities performing public tasks[14], together with the connections between them and relations with users"[15].

[9] System bezpieczeństwa cyberprzestrzeni RP, NASK/CERT Polska, s. 62, Warszawa, wrzesień 2015 r. <https://mac.gov.pl/files/nask_rekomendacja.pdf>.

[10] Zob. więcej na ten temat: K. Chałubińska-Jentkiewicz, *Cyberprzestępczość jako paradygmat pojęcia bezpieczeństwa w cyberprzestrzeni*, „Wojskowy Przegląd Prawniczy" 2016, nr 3, s. 46–64.

[11] Dz.U. nr 222, poz. 1323.

[12] Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. nr 156, poz. 1301).

[13] Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. nr 113, poz. 985)

[14] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. nr 64, poz. 565).

[15] Art. 2 ust. 1a ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym.

The same legal definition is contained in the Act of 18 April 2002 on the state of natural disaster[16]. These laws apply to virtual reality in which legal entities move when martial, emergency or natural disaster states take place. The concept of the national cyber security system adopted in the Assumptions of the Cybersecurity Strategy of the Republic of Poland includes, inter alia, rebuilding the definition of cyberspace and its extension to the sphere of key operators functioning in the economic sphere.

The concept of cyberspace can therefore be defined as a synthesis of all physical and technical means which enable the exchange information electronically as well as the relationships of its users having access to its resources.

Cybersecurity or network security is a term referring to providing protection and counteracting threats that affect cyberspace itself as well as functioning of subjects in cyberspace in both public and private sectors as well as their mutual relations. However, according to Act 2 point 4 of the Act of 5 July 2018 on the national cyber security system[17] – cybersecurity means the resistance of information systems to activities violating the confidentiality, integrity, availability and authenticity of processed data or related services offered by these systems. Therefore, this definition comprises the issues of technical nature and network protection as such. On the other hand, in favour of this position, one can also find the definition of cybersecurity in much broader, interdisciplinary perspective including all incidents which occur in cyberspace [18]. The incident pursuant to art. 2 point 5 of the Act on the national cybersecurity system is an incident – an event which has or may have an adverse effect on cybersecurity. However, according to art. 2 point 6 a critical incident is an incident resulting in significant damage to safety or public order, international affairs, economic benefits, public institutions activities, law and civic rights and freedoms as well as to people's life and health properly classified by the appropriate CSIRT MON, CSIRT NASK or CSIRT GOV.

[16] Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. nr 62, poz. 558).

[17] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560).

[18] Zaznaczyć także trzeba, że jednym z wciąż podstawowych problemów dotyczących odpowiedzialności w sieci jest zagadnienie jurysdykcji terytorialnej, która znalazła zastosowanie w przepisach Konwencji o cyberprzestępczości. Problemy z ustaleniem osoby przestępcy, a jak wiadomo większość przestępstw popełnianych jest w innych państwach niż faktyczne miejsce przebywania przestępcy, utrudnia działania związane z efektywnością ścigania cyberprzestępczości.

To go into further distinction of incidents, we can talk about a major incident which is an incident that causes or may cause a serious reduction in quality or interruption of the key service provision; crucial incident – an incident that has a significant impact on the provision of a digital service within the meaning of Art. 4 of Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for the application of Directive (EU) 2016/1148 of the European Parliament and of the Council with regard to further clarifying the elements to be taken into account by digital service providers in managing existing risks for the security of network and information systems, and parameters to determine whether an incident has a significant impact, hereinafter referred to as "Implementing Regulation 2018/151"[19].

An incident in a public entity -an incident that causes or may cause a reduction in quality or interruption of the implementation of a public task being carried out – these are activities that enable detection, recording, analyzing, classifying, prioritizing, taking corrective actions and reducing the effects of an incident.

The whole complexity of these issues parallels the issues happening in the real world. Thus, the legislators at various levels, both international and national, are introducing new regulations. In consequence, any kind of the phenomenon of impunity for illegal activities is no longer possible on the net. It should be noted that cyberspace in terms of adopting or creating new rules of behaviour is more flexible than reality. This unique ability of cyberspace brings comfort and completely new challenges to the legislator. The convenience is the ease of introducing regulations adequate to those in force in the real world, but the provisions so established often face blocking or ordinary ignorance on the part of ICT network users, in particular due to the lack of instruments for pursuing claims or prosecuting crime. One of the key problems is to identify entities responsible for ensuring cybersecurity, entities responsible for illegal activities on the network, mainly related to the provision of services, and for undesirable effects that are the result of computer activity. These three areas determine three directions of research related to responsibility in cyberspace.

Cyberspace is nowadays a symbol of development, but also freedom and privacy, and every interference in its functioning is associated with an attack on these values. In the countries involved in building the information society, cyberspace security is recognized as one of the most serious challenges in

[19] Odpowiedzialność w cyberprzestrzeni RP (Dz.Urz. UE L 26, s. 48).

the national security system. It refers to both the security of the entire state institution and individual citizens. That is why public tasks for cyberspace security occupy an important place in the National Security System of the Republic of Poland. The responsibility for ensuring cybersecurity rests with all network users, but with no doubt, public administration bodies play a crucial role in providing actions to ensure public security and order.

As previously mentioned, one of the priority public tasks is to ensure the security of cyberspace as a cross-sectoral area. Cybersecurity is important because threats in cyberspace can negatively affect national needs, and their implementation is the essence of public tasks. The most important national needs include: systematic needs (e.g. strengthening of the socio-economic system and legal order), economic needs (e.g. development of the country, economic growth), social needs (ensuring health protection, social security, and counteracting all forms of discrimination), ecological needs (environmental protection) and cultural needs (nurturing national heritage, respecting ideological and ethnic differences) [20]. All possible cyber threats can affect each of these national needs negatively and it explains why cyberspace security is so important for the proper functioning of the state. Public tasks in the field of cyberspace security are implemented primarily through the cooperation of public authorities and services responsible for cybersecurity both at the national (private sector, non-governmental organizations) and international (NATO, European Union, UN, transnational associations)[21]. Another important element of these tasks are legislative activities, i.e. the preparation of appropriate legal provisions protecting cyberspace and thus reducing the risk of potential attacks[22]. The strategic tasks in the field of cyberspace security include: combating threats in cyberspace; protection of state information systems; cooperation with the private sector (mainly telecommunications) in the scope of providing information on cyber threats; proactive and preventative actions in the field of citizens' security against cyber threats; tracking cyber crimes and prosecuting their perpetrators; conducting both offensive and defensive information activities in cyberspace,

[20] W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system*, Warszawa 2011, s. 37.

[21] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2006, s. 244.

[22] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2012, s. 21.

as well as cooperation with other entities of the National Security System of the Republic of Poland[23].

Thus, various types of state entities, guards, services and inspections reporting to the Prime Minister or individual ministers are obliged to fulfil public tasks in order to maintain cyber safety. The leading role among them, due to their competences, is played by the Internal Security Agency, the Minister of Digitization, the Minister of the Interior and Administration and the Minister of National Defense. There are also many other public authorities responsible for this zone, such as the President of the Office of Competition and Consumer Protection.

However, the Minister of National Defense plays a key role in the security of cyberspace. With the development of digitization of public administration, the Armed Forces have also undergone the process of computerization and as a result, it led to the emergence of sensitive points vulnerable to attacks from cyberspace[24]. New technologies and networks are used more and more often in operational reconnaissance[25] or information struggle. These processes are intensifying with the development of nanotechnology and automated and robotic devices. It should be noted that offensive operations also penetrate cyberspace, which means that more countries are deciding to develop digital offensive capabilities designed to deter potential aggressors[26]. Changes related to digitization resulted in the creation of special units dealing with cyberspace security in the structures of the Polish Armed Forces. As part of the General Staff of the Polish Army, under the leadership of the General Commander of the Armed Forces, there is the Information Systems Inspectorate connecting individual IT support units that operated until October 1, 2013. The creation of the Information Systems Inspectorate clarified the responsibility for the IT security management system in cyberspace, which is the responsibility of the Minister of National Defence. The General Staff of the Republic of Poland performs other tasks in the field of cyberspace security with the help of the Command and Communications Systems Planning Board. The newly created unit reporting to the Ministry of National Defence is the National

[23] Biała księga bezpieczeństwa narodowego Rzeczypospolitej Polskiej, Warszawa, 2013, s. 250, <http://www.spbn.gov.pl/>, s. 63.

[24] P. Bączek, *Zagrożenia…*, s. 136.

[25] M. Sadlok, *Cyberterroryzm, cyberprzestępczość – wirtualne czy realne zagrożenie?*, <http://www.racjonalista.pl/kk.php/s,846>.

[26] M. Grzelak, K. Lidel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22, s. 128.

Cryptology Center, which deals with research and implementation of cryptographic solutions for the needs of the Polish public administration and the army. The Cybernetic Operations Center is being created as part of the National Cryptology Centre. Another important body that performs tasks to ensure the security of cyberspace is the President of the Office of Electronic Communications, which is a regulatory body in the field of telecommunications and postal services, and NASK which is responsible for cyber security. As a consequence of the development of these services, the Minister of Internal Affairs plays an extremely important role for cybersecurity and public order in cyberspace and the Chief Commander of Police plays a key role under the supervision of the former. There is a special department within the Headquarters of Police called the Support Unit for Fighting Cybercrime and it deals with internet crime detection, analysis of cyberspace incidents, exchange of information and cooperation with national and international subjects.

Moreover, it should be pointed that telecommunication entrepreneurs and network operators need new regulations in their work as well. It is hard to deny that the ability to monitor transactions and activities carried out by network users and to get information about financial operations, commercial behavior and decisions, consumer habits, etc. poses a serious threat to privacy, personal data protection, and generally a sense of security of the individual. The global extent of the telecommunication services contributes to the lack of full legal regulations in this area. Due to the fact that this type of services is cross-border hence local, national legal systems are not always valid in other countries. Furthermore, the market of telecommunication services is very different from traditional service market and that is why it requires totally different, innovative attitude towards legal regulations. Digital service market does not have the subsidiary character any longer in comparison to traditional service market because the internet became a crucial element of economic life and an important tool in the process of globalization of the services. Thus, new legal problems in electronic commerce "appeared as soon as the initial naïve belief (or hope) developed that most of the internet would be a kind of freedom without rigid legal frameworks, administrative restrictions or fiscal burdens"[27].

[27] J. Barta, R. Markiewicz, *Wstęp* [w:] J. Barta, R. Markiewicz (red.), *Handel elektroniczny. Problemy prawne*, Kraków 2005, s. 10.

Thus, it can be said that in recent years we have observed an increase in public administration's interest in cyberspace security, which means that more and more units and organizations dealing with this problem are being created. However, for more effective performance of public tasks in this area, cooperation and exchange of information between administrative, military and civilian areas is necessary. The European Union Cybersecurity Strategy: open, secure and protected cyberspace[28] proposes the creation of a network of national cybersecurity authorities. According to the EU strategy, national network and information security authorities should cooperate and exchange information with other regulatory authorities, in particular with personal data protection authorities, and regularly publish non-classified information on current early incidents and threats on a dedicated website and coordinated responses. According to the European Commission, legal obligations should not replace or prevent informal and voluntary cooperation, including cooperation between the public and private sectors, aimed at increasing the level of security and the exchange of information and best practices. A particularly important and useful platform at EU level to be developed is the European Public-Private Partnership on Resilience[29].

The above-mentioned tasks of public entities, however, do not make the list of necessary conditions related to the protection of national security in the digital age. However, responsibility for online activities has a cross-sectoral dimension. In the EU strategy "Cybersecurity strategy of the European Union: open, secure and protected cyberspace", which the European Commission published on February 7, 2013 as a joint communication of the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – "The European Union Cybersecurity Strategy: Open, secure and protected cyberspace", it was found that private entities still lack effective incentives to provide reliable data on incidents in terms of network and information security and their effects, to the system speech prevention and to invest in security solutions. The purpose of the proposed legal act is therefore to bring about a situation in which entities operating in

[28] COM (2013) z 7 lutego 2013 r. JOIN(2013) 1 final.

[29] Europejskie partnerstwo publiczno-prywatne na rzecz odporności zostało zainicjowane na podstawie dokumentu COM(2009) 149. Platforma ta zainicjowała działania i intensywniejszą współpracę między sektorem publicznym i sektorem prywatnym w zakresie identyfikacji kluczowych zasobów, środków, funkcji i podstawowych wymogów w odniesieniu do odporności, jak również zapotrzebowania na współpracę i mechanizmy reagowania na zakrojone na szeroką skalę zakłócenia łączności elektronicznej.

many key areas (energy, transport, banking, stock exchanges, technologies enabling the provision of key internet services, as well as public administration bodies) assess cybersecurity threats, based on which are exposed, ensure the reliability and resilience of networks and information systems using appropriate threat prevention strategies, and exchange information with relevant network and information security authorities. Systemic prevention of threats in the field of cybersecurity can contribute to increasing economic opportunities and competitiveness in the private sector, making cybersecurity one of the advantages of the services offered. These entities will be required to report incidents to the competent national authorities on network security and information that have a significant impact on the continuity of basic services and the supply of goods dependent on networks and information systems.

The strategy highlights the need to promote dialogue and coordination between civil and military subjects in the EU, placing particular emphasis on the exchange of good practices, exchange of information, early warnings, response to incidents, threat assessment, information activities, and making cybersecurity a priority; ensuring dialogue with international partners, including NATO, and with other international organizations and multinational centers of excellence to ensure effective defense capabilities, identify areas of cooperation and avoid duplication of efforts.

According to the European Commission, the responsibility for increasing security in cyberspace rests with all entities that create the global information society, from citizens to government administrations. The EU supports actions aimed at defining norms of behavior in cyberspace to which all interested parties should comply. Just as the EU expects citizens to comply with civil and social norms and online law, states should also comply with applicable norms and regulations. In matters of international security, the EU encourages support for actions to build confidence in cybersecurity to increase transparency and reduce the risk of false perceptions of your actions. The legal obligations contained in the International Covenant on Civil and Political Rights, the European Convention on Human Rights and the EU Charter of Fundamental Rights should also be respected online. The EU will focus on how to ensure that these obligations are also enforced in cyberspace. As regards the fight against cyber crime, the Budapest Convention, which is open for adoption by third countries, is an appropriate instrument. It is a model for national legislation in the field of cybercrime and is the basis for international cooperation in this field. If armed conflicts extend to cyberspace, international humanitarian law and human rights law will apply.

Directive 2016/1148 is the first EU law in the field of cybersecurity introducing cross-sectoral regulations. The time to implement the directive in the legal systems of the member states expired on May 9, 2018. The text of the directive focuses on three pillars: 1) institutions that should be established in all Member States; 2) cooperation at European level; 3) obligations regarding network and information security.

Under the first pillar, each Member State is required to establish competent authorities for network and information security, which are responsible for monitoring the application of its provisions in sectors falling within its scope. Due to differences in national management structures, Member States may designate more than one national competent authority responsible for performing cybersecurity tasks of key service operators and digital service providers.

In the above context, new obligations of the so-called: key service operators should be looked at. “Key service” means a service that is critical to maintaining critical social or economic activities as listed in the list of key services. The operator of the key service is the entity referred to in Annex No. 1 to the Act on the national cybersecurity system, having an organizational unit on the territory of the Republic of Poland, towards which the authority competent for cybersecurity issues made a decision regarding the recognition of the key service operator. Sectors, subsectors and types of entities are set out in Annex 1 to the Act. The competent authority for cybersecurity makes a decision on the recognition of an entity as a key service operator, if: 1) the entity provides the key service; 2) the provision of this service depends on information systems; 3) the incident would have a significant disruptive effect on the provision of the key service by that operator.

The subjective scope of the directive has been formulated in two formulas: operators of key services and digital service providers. Different requirements apply to the operators indicated in each of the annexes. For digital service providers (Annex III), a gentle and reactive approach is required to cover ex-post supervisory activities, i.e. after the incident and only by the country where the service provider is located. Thus, entities from Annex III will not be subject to the previously described identification or reporting process, as in the case of key service operators. This approach is due to the international dimension of operators providing digital services, and thus the fear of fragmentation of the EU digital single market. As a result of negotiations, it was agreed that regulations would cover shopping websites, search engines and cloud services. The annex to the Act contains all potential categories of entities in individual sectors of the economy and the state's activity, from which operators of key services can be selected by administrative decision.

In Poland, the Act on the national cybersecurity system has assigned specific tasks to existing entities that deal with computer incident response as part of their activities.

CERT GOV

The Governmental Computer Incident Response Team CERT.GOV.PL acts as the main CERT team responsible for coordinating the process of responding to computer incidents occurring in the area ofgovernment administration and critical infrastructure. One of its basic tasks is recognizing, preventing and detecting threats to security – important from the point of view of the continuity of the state's functioning – ICT systems of public administration bodies or the ICT network system covered by a uniform list of objects, installations, devices and services included in the critical infrastructure, and also ICT systems of owners and holders of critical infrastructure facilities, installations or devices referred to in art. 5b paragraph 7 point 1 of the Crisis Management Act.

RON SRNIK

The Computer Defense Incident Response System of the Ministry of National Defense carries out tasks in coordinating the processes of preventing, detecting and responding to computer incidents in the ICT systems and networks of the Ministry of National Defense.

SRnIK RON is organized into a three-level structure in accordance with NATO assumptions (SRnIK Coordination Center, SRnIK Support Center, which carries out tasks in accordance with the scope of activities of the CERT Teams, and administrators of IT systems of RON units and organizational units).

The main tasks of SRnIK include coordination of response to computer incidents, handling and analysis of events and incidents, as well as conducting activities aimed at increasing awareness of ICT security.

As part of its tasks, SRnIK cooperates with organizational units and units of the Ministry of National Defense, as well as with non-departmental, national and international organizations.

National Center of Cybersecurity

In July 2016, the National Cybersecurity Center (NC Cyber) was established as part of NASK, designed as a center for rapid response to threats and reported incidents in cyberspace, and in the event of possible attacks – to take necessary actions in cooperation with centers in the country and abroad to analyze the nature, manner, extent of the incident, and to exchange information to alert key sectors and institutions. NC Cyber issues recommendations on how to deal with the threat and necessary actions to minimize the effects.

Public and private entities may cooperate with NC of Cybersecurity on the basis of signed agreements in the field of cybersecurity, they may also delegate their representatives to ongoing cooperation.

The Act sets out obligations for operators of key services regarding the implementation of an effective safety management system, including risk management, procedures and mechanisms for reporting and handling incidents or organization of structures at the operator level. In addition, the Act specifies the obligations imposed on digital service providers, taking into account the existing restrictions in this respect set out in Directive 2016/1148. First of all, it is assumed to define CSIRT tasks responsible for counteracting cybersecurity threats of cross-sectoral and cross-border nature, as well as to coordinate the handling of serious, significant and critical incidents. Secondly, the Act provides for the inclusion of cybersecurity aspects in the sphere of state management. In addition, the Act provides for the establishment of the Critical Incident Team as an auxiliary body appointed in the matters of service and coordination of the listed critical incidents at the national level of CSIRT and RCB.

The need for cross-sectoral cooperation results from the fact that the process of emergence of threats is continuous, therefore the list of incident response needs is constantly increasing and thus the list of entities responsible for cybersecurity is expanding. The right selection of legal instruments must meet these needs without negating the classic means. Digital democracy is a form of government activity in which public authorities and public administration bodies are required to counteract any negative trends for national security. However, it is important to stress the importance of NGOs in activities related to ensuring constantly growing cybersecurity.

Technological changes have also affected the scope of responsibility for criminal acts, but at the same time new rules have emerged related to the limitations of this responsibility. In the European law, the liability of online service providers is regulated by Directive 2000/31 / EC. This directive includes provisions related to the most popular network services: mere conduit, caching and hosting. It should be emphasized here that European regulation adopts a horizontal model. This means that the exclusions it provides apply to all legal liability, including civil, criminal and administrative liability. The e-commerce directive creates rules for exclusion of liability at the maximum level. Therefore, individual Member States may decide to introduce less restrictive solutions.

The implementation of the provisions of the Directive on electronic commerce in Polish law are art. 12–15 of Act on Provision of electronic services. In accordance with art. 12 of this Act, referring to the mere conduit service, if the person who by transmitting data: 1) is not the initiator of the transmission, 2) does not select the recipient of the data and 3) does not delete or modify the data being the subject of transmission, is not responsible for the information provided. The exclusion of liability referred to in paragraph 1 also includes the automatic short-term intermediate storage of transmitted data, if this action is only intended to carry out the transmission and the data is not stored longer than is normally necessary to carry out the transmission (caching, art. 12 section 2 of the Act on Provision of electronic services).

Therefore, respecting the integrity of stored data remains a necessary condition to avoid legal liability. In accordance with art. 13 section 2 of the Act on Provision of electronic services one shall not be liable for stored data who, under the conditions referred to in paragraph 1, immediately deletes the data or prevents the access to the stored data, when he receives a message that the data has been deleted from the initial transmission source or access to them has been prevented, or if the court or other competent authority ordered the deletion of data or preventing access to them, storage of data by the recipient, he is not aware of the unlawful nature of the data or related activities, and in the event of receiving official notification or obtaining reliable information about the unlawful nature of the data or related activities will immediately prevent access to this data.

In turn, Article 14 of Directive 2000/31 / EC should be interpreted as meaning that the rule laid down therein applies to the entity providing the internet referencing service if, when providing its services, the service provider does not play an active role which could cause him to have knowledge of stored information or have control over it. If the said service provider does not play such a role, he cannot be held liable for the content of information stored at the advertiser's request, unless, having become aware of the unlawful nature of this information or the advertiser's activity, he has not immediately taken appropriate action to remove the said information or prevent access to it .

The regulations listed here justify the thesis that in each case the responsibility of the same entity will be different depending on whether it conducts service activities referred to in the Act on the provision of electronic services, or is the sender or publisher. As a result of technological and economic convergence, the same entity can perform very different functions and it is not a foregone conclusion that its status, and thus the scope of responsibility, is finally established. This situation indicates the need to introduce appropriate regulations, subject to the need to synchronize issues at every stage of substantive legislative activities. This is an essential element in creating a coherent system of regulatory frameworks.

The document Cyberspace Protection Policy of the Republic of Poland states that cyberspace security is a set of organizational and legal, technical, physical and educational projects aimed at ensuring smooth functioning of cyberspace. In turn, a cyberattack is a deliberate disruption of the proper functioning of cyberspace, and cybercrime is a criminal act committed in the area of cyberspace[30]. These definitions were developed on the basis of actions to be taken in the digital domain. Thus, cybercrime is defined as a type of crime in which a computer is either a tool or an object of crime. This term covers all types of crimes that were committed with the participation of a computer or ICT networks or which were directed at these devices. However, the computer can also be the culprit. Therefore, the third area that requires a separate and expanded analysis of the responsibility associated with the functioning of cyberspace is the zone of computer operation. In 1997, Garri Kasparow, one of the world's greatest chess players, lost the game to the Deep Blue program – a specialized supercomputer programmed by IBM and constructed for the price of $ 10 million.

[30] Online <file:///C:/Users/kjentkiewicz/Downloads/Polityka_Ochrony_Cyberprzestrzeni_RP_148x210_wersja_pl.pdf>, s. 5, MAiC ABW.

The ability of computers to analyze and solve problems, also in the area of ethics, creates interesting issues regarding the answer to the questions, what is moral and what is immoral, what is good and what is evil, what is allowed and what should be banned in legal approach. These dilemmas are a basic element in determining the degree of responsibility. If we assume that computers are increasingly independent in thinking and decision-making, can it be assumed that they are also aware of the existence of morality? Can the concept of morality be considered by the machine and do computers have morality and is it imposed or their own? This seems to be the key to answering questions related to responsibility for cyberspace activities. The courts try to attribute responsibility for damages caused to people by artificial intelligence machines. Does artificial intelligence have any legal entity or does it have the capacity to perform legal acts? Can computers be responsible for their actions? It seems to be a matter of having legal entity. In various positions of law theorists, such as, for example, Ugo Pagallo, the author of The Law of Robots, proves that we should distinguish between the behavior of robots as tools for interpersonal interaction and as entities in the legal sphere.

It seems a matter of time for an artificial intelligence-led computer to be responsible for the caused damage. Judge Curtis Karnow proposes the creation of a legal entity which he describes as "electronic personality". Although the producers of artificial intelligence will escape the responsibility for its actions after manufacturing the robot, it seems that they will still be responsible under the warranty. The legal doctrine of cyber responsibility will be particularly important in the face of changes in life, in the conditions of the development of artificial intelligence. Today, the principles of responsibility are also defined by the distinction between hardware and software, also in the sphere of law. The potential danger posed by artificially intelligent machines increases when they become mobile. Designing technologies or techniques of artificial intelligence and cyborgs will be important in creating a future in which artificial intelligence will loyally and ethically work for a human being. Of course, the law can always regulate the issues of criminal or civil liability for misconduct, prohibited acts, but the dynamics of the development of artificial intelligence and robotics far exceed the possibilities of regulators and legislators. Under these circumstances, ethical principles and morals dictated by public morals will still be heard.

The concept of online security or cyber security consists of resources protection – data, information, digital content in general, the protection of ICT networks and the protection of content transmission via the network, and thus the communication process itself. From the specifics of the operation of the network it follows – if we theoretically assume that antivirus software and firewalls do their job – that, like a virus vaccine, they will not work in the event of new threats or modifications of those already known.

Therefore, the process of regulating cyberspace is a multi-stage task, requiring constant monitoring of various socially adverse effects. This also applies to the functioning of machines.

To sum up, it should be noted that today the chess master is not a human or a machine, but a team of people and computers. Computers are still performing activities that they have been programmed for but they lack intuition and creativity. Fortunately, people are strong in what computers are weak at, and this creates a potential partnership.

As Freeman Dyson (1988) said: "technology is God's gift. This is probably the greatest gift after a gift of life. She is the mother of civilization, arts and sciences".

Bibliography

Literature

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2006, s. 244.

Barta J., Markiewicz R., *Wstęp* [w:] J. Barta, R. Markiewicz (red.), *Handel elektroniczny. Problemy prawne*, Kraków 2005.

Chałubińska-Jentkiewicz K., *Cyberprzestępczość jako paradygmat pojęcia bezpieczeństwa w cyberprzestrzeni*, „Wojskowy Przegląd Prawniczy" 2016, nr 3.

Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii*, Warszawa 2015.

Goban-Klas T., *Cywilizacja medialna*, Warszawa 2005.

Grzelak M., Lidel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22.

Kitler W., *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system*, Warszawa 2011.

Siwicki M., *Nielegalna i szkodliwa treść w Internecie. Aspekty prawno-karne*, Warszawa 2011.

Suchorzewska A., *Ochrona prawna systemówin formatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2012.

Legal acts

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. nr 156, poz. 1301).

Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. nr 113, poz. 985).

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. nr 64, poz. 565).

Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. nr 62, poz. 558).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560).

Odpowiedzialność w sieci – wstęp do problematyki

Streszczenie

Artykuł odnosi się do diagnozy obecnego stanu prawnego w przedmiocie odpowiedzialności w obszarze cyberprzestrzeni, który sam w sobie jest trudny do zdefiniowania. Polskie rozwiązania ustawowe, strategiczne i programowe przygotowywane są w warunkach standardów UE. Analiza obejmuje przegląd zagrożeń (głównie związanych z infrastrukturą informacyjną i teleinformatyczną) i ich uwarunkowań (systemowych, ekonomicznych, społeczno-kulturowych). Istotną kwestią jest ustalenie adresatów zobowiązanych do działań zapobiegawczych i eliminacyjnych (przede wszystkim władz publicznych, ale także innych, np. podmiotów komercyjnych lub przedstawicieli działających na rynku społeczeństwa informacyjnego). Odpowiedzialność za działania w sieci dotyczy także kwestii współpracy merytorycznej i instytucjonalnej na poziomie europejskim.

Słowa kluczowe: cyberprzestrzeń, cyberbezpieczeństwo, odpowiedzialność, zagrożenia, społeczeństwo informacyjne, infrastruktura informacyjna, infrastruktura teleinformatyczna, komunikacja, nowe technologie