Public Entities within the National Cybersecurity System and their Responsibilities

JAROSŁAW KOSTRUBIEC

Abstract The national cybersecurity system relies fundamentally on the public entities which have been given the mission of safeguarding the uninterrupted provision of cyberspace services. They have also been assigned with important tasks related to handling incidents, i.e. events which have, or may have, an adverse impact on cybersecurity. Events in cyberspace are extremely dynamic, making it necessary to constantly monitor the processes taking place there. Legal solutions should be in place to pre-empt these dynamic events. Hence the legislators are tasked with developing legal mechanisms to prevent, counteract, and eliminate the consequences of such undesirable phenomena. Accordingly, the legislators decided to regulate the organisation of the national cybersecurity system and the tasks and responsibilities of entities within this system, as well as the procedure for supervising and inspecting cybersecurity in order to allow relevant entities to respond appropriately to cyberspace threats.

Keywords: • public entities • cybersecurity • clasified information • responsibility

.

CORRESPONDENCE ADDRESS: Jarosław Kostrubiec, Ph.D., Dr. Habil. Associate Professor, Maria Curie-Skłodowska University (Lublin), Faculty of Law and Administration, Plac Marii Curie-Skłodowskiej 5, 20-031 Lublin, Poland, email: j.kostrubiec@umcs.pl.

https://doi.org/10.4335/2021.5 ISBN 978-961-7124-03-3 (PDF)
Available online at http://www.lex-localis.press.

1 Entities within the national cybersecurity system

The national cybersecurity system is comprised of a number of public entities with a different legal and territorial status, as well as non-public entities, including those which perform public tasks. However, it is public entities, in particular those which specialise in cybersecurity, that play a fundamental role in this system, although other entities should not be ignored.

In accordance with Article 3 of the National Cybersecurity System Act of 5 July 2018 (consolidated text, Polish Journal of Laws of 2020, item 1396, as amended – NCSA), the objective of the national cybersecurity system is to ensure cybersecurity at the national level, including the uninterrupted provision of essential services and digital services by achieving the appropriate level of security of the information systems used to provide these services and ensuring the handling of incidents. And this objective will guide the operations of public entities within this system. The term cybersecurity encompasses the protection of resources – data and information, i.e. digital content – ICT networks, devices, and the protection of content transmission on the Internet (Chałubińska-Jentkiewicz, 2019: 20).

Entities within the national cybersecurity system are defined in Article 4 of the NCSA, and these include: 1) operators of essential services; 2) digital service providers; 3) CSIRT MON (the Computer Security Incident Response Team of the Ministry of National Defence); 4) CSIRT NASK (the Computer Security Incident Response Team of the National Research Institute NASK); 5) CSIRT GOV (the Computer Security Incident Response Team of the Internal Security Agency); 6) sectoral cybersecurity teams; 7) selected public-finance sector entities; 8) research institutes; 9) the National Bank of Poland; 10) Bank Gospodarstwa Krajowego (BGK – a Polish national development bank); 11) the Office of Technical Inspection (UDT); 12) the Polish Air Navigation Services Agency; 13) the Polish Centre for Accreditation; 14) the National Fund for Environmental Protection and Water Management and regional funds for environmental protection and water management; 15) companies and partnerships (as governed by the Polish Code of Commercial Companies and Partnerships (PCCCP)) performing tasks of a public utility nature; 16) entities providing cybersecurity services; 17) competent authorities for cybersecurity; 18) the Single Point of Contact for cybersecurity; 19) the Government Plenipotentiary for Cybersecurity; 20) the College for Cybersecurity.

Under Article 5 of the NCSA, operators of essential services are entities referred to in Annex 1 to the NCSA whose organisational units are located within the territory of the Republic of Poland and which have been recognised by the competent authority for cybersecurity as operators of essential services through a decision to that effect.

Digital service providers are defined by Article 17 of the NCSA, pursuant to which they are legal persons or non-corporate organisational units which have their head office, or

whose management board is based, within the territory of Poland, or whose representative has an organisational unit in Poland, which provide digital services, except for micro- and small enterprises.

Article 2 (2) of the NCSA stipulates that CSIRT MON is the Computer Security Incident Response Team which operates at the national level and is led by the Minister of National Defence.

In accordance with Article 2 (3) of the NCSA, CSIRT NASK is the Computer Security Incident Response Team which operates at the national level and is led by NASK – the Research and Academic Computer Network – the National Research Institute.

As per Article 2 (1) of the NCSA, CSIRT GOV is the Computer Security Incident Response Team which operates at the national level and is led by the Head of the Internal Security Agency.

Pursuant to Article 44 (1) of the NCSA the competent authority for cybersecurity may appoint a sectoral cybersecurity team for a given sector or subsector to be responsible in particular for: 1) receiving serious-incident reports and supporting the handling of serious incidents; 2) supporting operators of essential services in the fulfilment of their specific responsibilities; 3) analysing serious incidents, finding links between incidents and formulating conclusions from incident handling; 4) cooperating with the relevant CSIRT MON, CSIRT NASK and CSIRT GOV in coordinating serious-incident handling.

Selected public finance sector entities within the national cybersecurity system include: 1) public authorities, including government administration authorities, state inspection and legal protection authorities, and courts and tribunals; 2) local government units and their unions (Kostrubiec, 2020; 188-191); 3) metropolitan unions (Bosiacki & Kostrubiec, 2018: 364-365); 4) budgetary units; 5) local government-owned budgetary establishments; 6) executive agencies; 7) public sector enterprises; 8) the Social Insurance Institution and the Funds under its management, and the Agricultural Social Insurance Fund and the Funds managed by the President of the Agricultural Social Insurance Fund; 9) the National Health Fund; 10) public higher education institutions; 11) the Polish Academy of Sciences and the organisational units established by it.

Article 1 of the Act of 30 April 2010 on Research Institutes (consolidated text, Polish Journal of Laws of 2020, item 1383, as amended) stipulates that a research institute is a state organisational unit which is legally, organisationally and financially separate, and which conducts research, as well as development work towards the implementation and practical application of such research. An institute acquires a legal personality upon its entry into the National Court Register, and it has the right to use a round seal with the national emblem of the Republic of Poland in the middle and its name in the rim.

The National Bank of Poland (NBP) is the central bank of the Republic of Poland. Its primary purpose is to maintain stable price levels while supporting the economic policy of the Council of Ministers, provided that this does not restrict its core purpose. This purpose is defined by Article 1 and Article 3 (1) of the Act of 29 August 1997 on the National Bank of Poland (consolidated text, Polish Journal of Laws of 2019, item 1810, as amended).

Bank Gospodarstwa Krajowego (BGK) is a state-owned bank, as explicitly stipulated by Article 2 (1) of the Act of 14 March 2003 on Bank Gospodarstwa Krajowego (consolidated text, Polish Journal of Laws of 2020, item 1198). A state-owned bank may be established or liquidated by the Council of Ministers by way of a resolution – Article 14 (1) of the Act of 29 August 1997 – Banking Law (consolidated text, Polish Journal of Laws of 2019, item 2357, as amended). BGK has a legal personality and conducts its activities on the territory of the Republic of Poland, including through its organisational units. BGK's activities outside the Republic of Poland serve to ensure the achievement of its core objectives and tasks, as stipulated by § 3 of BGK's Charter granted by the Regulation of the Minister of Economic Development of 16 September 2016 on Granting a Charter to Bank Gospodarstwa Krajowego (Polish Journal of Laws of 2016, item 1527, as amended).

The Office of Technical Supervision is a technical supervision entity established as a state-owned legal person. This status is defined by Article 35 (1) of the Act of 21 December 2000 on Technical Supervision (consolidated text, Polish Journal of Laws of 2019, item 667, as amended).

The legislators have established the Polish Air Navigation Services Agency as a state-owned legal person which may form its local branches – Article 1 of the Act of 8 December 2006 on the Polish Air Navigation Services Agency (consolidated text, Polish Journal of Laws of 2017, item 1967, as amended).

The Polish Centre for Accreditation is a national accreditation body which acts as a legal person and is supervised by the competent minister for the economy – Article 38 of the Act of 13 April 2016 on Conformity Assessment and Market Surveillance Systems (consolidated text, Polish Journal of Laws of 2019, item 544, as amended). The national accreditation body operates on a non-profit basis and does not offer or provide any activities or services that conformity assessment bodies provide, and it does not provide consultancy services, own shares in, or otherwise have a financial or managerial interest in a conformity assessment body. Each Member State ensures that its national accreditation body has the appropriate financial and personnel resources for the proper performance of its tasks, including the fulfilment of special tasks, such as activities for European and international accreditation cooperation and activities that are required to support public policy and which are not self-financing. This scope is defined by Article 4 of Regulation (EC) No. 765/2008 of the European Parliament and of the Council of 9 July

2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No. 339/93 (OJ EU L 2018, p. 30).

The National Fund for Environmental Protection and Water Management and regional funds for environmental protection and water management are environmental institutions. The former is a state-owned legal person and the latter are local government-owned legal persons, as stipulated by Article 386 (3) and Article 400 of the Act of 27 April 2001 – Environmental Protection Law (consolidated text, Polish Journal of Laws of 2020, item 1219, as amended). The National Fund for Environmental Protection and Water Management is a state-owned earmarked fund. This fund is an administrative entity of a functional nature, given some of its statutorily assigned public tasks relating to its being the administrator of the money provided to that fund, as described in the Judgement of the Supreme Administrative Court of 15 March 2016, II OSK 1465/15 (LEX No. 2037370). In light of the Judgement of the Provincial Administrative Court of 13 July 2010, II SA/OI 345/10 (LEX No. 738170), regional funds for environmental protection are not local government units, and as such they are not established by the Province, but by way of an Act, and it is not the obligation of provinces to provide them with assets. As a result of the link between the operations of provincial funds and the Public Finance Act, these funds operate as public finance sector entities whose purpose is to perform tasks identified in the budget and arising explicitly from the Act under which these entities are established. As such they are not provincial organisational units, since provincial funds represent separate organisational entities which have their legal personality and operate alongside these units.

The national cybersecurity system also comprises partnerships and companies performing tasks of a public utility nature. Through a partnership agreement or articles of association the partners or shareholders assume the obligation to pursue a common objective by making contributions and, if the partnership agreement or articles of association so provide, cooperating in a different, specific manner – Article 3 of the Act of 15 September 2000 – Code of Commercial Companies and Partnerships (consolidated text, Polish Journal of Laws of 2020, item 1526, as amended). In light of the Judgement of the Appellate Court of 15 November 2017, I ACa 543/17 (LEX No. 2488258), it is beyond any doubt that a partnership agreement or articles of association must be defined as a legal relationship of an at least bilateral nature, established between the partners or shareholders. Article 1 (2) of the Act of 20 December 1996 on Municipal Services (consolidated text, Polish Journal of Laws of 2019, item 712, as amended) stipulates that the performance of tasks of a public utility nature serves to ensure the ongoing and uninterrupted fulfilment of the collective needs of the population through the provision of publicly available services.

Providers of cybersecurity services are digital service providers (providers of services by electronic means) – the provision of a service by electronic means involves the rendering

of a service without the parties being present at the same time and in the same place – i.e. remotely – through the transmission of data at an individual request of the service recipient, sent and received with the use of electronic processing equipment, including digital compression, and data storage, being sent, received or transmitted entirely through the telecommunications network, as stipulated by Article 2 (4) of the Act of 18 July 2002 on the Provision of Services by Electronic Means (consolidated text, Polish Journal of Laws of 2020, item 344), or providers of essential services (in accordance with the legal definition set out in Article 2 (16) of the NCSA, an essential service is a service which is essential to maintaining critical social or economic activities, as provided in the list of essential services. A digital service is: 1) a service which enables consumers or businesses to conclude, by electronic means, contracts with businesses on the website of an online marketplace or the website of a business which uses services provided by an online marketplace; 2) a service which allows access to a scalable and flexible set of computing resources for common use by multiple users; 3) a service which allows users to find all websites, or websites in a specific language, using queries comprising a key word, expression or other element, and which produces results in the form of links to information related to the query. As digital services continue to evolve rapidly. so do threats associated with access to information by unauthorised entities. Therefore, the technological development associated with digitisation must go hand in hand with the advancements in the use of appropriate safeguards to prevent unauthorised access to information held by authorised entities. It is imperative for the digitisation process to be integral to the process of ensuring information security, and a proportionate relationship must exist between them. The development of advanced technologies must coincide with advancements in the system of safeguards (Karpiuk, 2014; 33).

In accordance with Article 41 of the NCSA the competent authorities for cybersecurity are: 1) for the energy sector – the minister competent for energy; 2) for the transport sector, excluding the water transport subsector – the minister competent for transport; 3) for the water transport subsector – the minister competent for the maritime economy and the minister competent for inland navigation; 4) for the banking sector and financial-market infrastructure sector – the Polish Financial Supervision Authority (KNF); 5) for the healthcare sector (excluding: a) entities subordinate to and supervised by the Minister of National Defence, including entities whose communication and information systems or ICT networks are included in the uniform list of facilities, installations, devices, and services which comprise critical infrastructure, b) enterprises of special economic and defence importance in respect of which the Ministry of National Defence is the authority organising and supervising the performance of tasks for state defence) – the minister competent for health; 6) for the healthcare sector comprising: a) entities subordinate to and supervised by the Minister of National Defence, including entities whose communication and information systems or ICT networks are included in the uniform list of facilities, installations, devices, and services which comprise critical infrastructure, b) enterprises of special economic and defence importance in respect of which the Ministry of Defence is the authority organising and supervising the performance of tasks for state

defence – the Minister of National Defence; 7) for the drinking water supply and distribution sector – the minister competent for water management; 8) for the digital infrastructure sector (excluding: a) entities subordinate to and supervised by the Minister of National Defence, including entities whose communication and information systems or ICT networks are included in the uniform list of facilities, installations, devices, and services which comprise critical infrastructure, b) enterprises of special economic and defence importance in respect of which the Ministry of National Defence is the authority organising and supervising the performance of tasks for state defence – the Minister of National Defence) – the minister competent for computerisation; 9) for the digital-infrastructure sector comprising: a) entities subordinate to and supervised by the Minister of National Defence, including entities whose communication and information systems or ICT networks are included in the uniform list of facilities, installations, devices, and services which comprise critical infrastructure, b) enterprises of special economic and defence importance in respect of which the Ministry of National Defence is the authority organising and supervising the performance of tasks for state defence; 10) for digital service providers (excluding: a) entities subordinate to and supervised by the Minister of National Defence, including entities whose communication and information systems or ICT networks are included in the uniform list of facilities, installations, devices, and services which comprise critical infrastructure, b) enterprises of special economic and defence importance in respect of which the Ministry of National Defence is the authority organising and supervising the performance of tasks for state defence;) – the minister competent for computerisation; 11) for digital service providers comprising: a) entities whose communication and information systems or ICT networks are included in the uniform list of facilities, installations, devices, and services which comprise critical infrastructure, b) enterprises of special economic and defence importance in respect of which the Ministry of National Defence is the authority organising and supervising the performance of tasks for state defence – the Minister of National Defence.

The Single Point of Contact for cybersecurity is managed by the minister competent for computerisation.

Pursuant to Article 60 of the NCSA the coordination of measures and government policies related to ensuring cybersecurity in the Republic of Poland is assigned to the Government Plenipotentiary for Cybersecurity. In accordance with Article 61 of the NCSA the Government Plenipotentiary for Cybersecurity is appointed and dismissed by the President of the Council of Ministers. The Plenipotentiary is either a minister, a secretary of state or an under-secretary of state, and he or she is subordinate to the President of the Council of Ministers. Substantive, legal, organisational, technical, and administrative support is provided to the Government Plenipotentiary for Cybersecurity by the ministry, or other government administration agency, which has appointed the Plenipotentiary.

The Council of Ministers has a College for Cybersecurity under its authority which acts as an opinion-giving and advisory body on cybersecurity matters and activities to CSIRT

MON, CSIRT NASK, CSIRT GOV, sectoral cybersecurity teams and competent authorities for cybersecurity. This status is given under Article 64 of the NCSA.

2 The responsibilities of public entities within the national cybersecurity system

The responsibilities of these public entities are set out in Chapter 5 of the NCSA, and apply to: 1) selected public finance sector entities; 2) research institutes; 3) the National Bank of Poland; 4) Bank Gospodarstwa Krajowego; 5) the Office of Technical Inspection (UDT); 6) the Polish Air Navigation Services Agency; 7) the Polish Centre for Accreditation; 8) the National Fund for Environmental Protection and Water Management, and regional funds for environmental protection and water management; 9) companies and partnerships performing tasks of a public utility nature – public entities.

Under Article 21 of the Commune Government Act a public entity performing a public task which depends on an information system is responsible for appointing a person in charge of maintaining contacts with entities within the national cybersecurity system. A public administration authority may appoint one person in charge of maintaining contacts with entities within the national cybersecurity system in relation to public tasks which depend on information systems and which are performed by entities subordinate to or supervised by that authority. A local government unit may appoint one person in charge of maintaining contacts with entities within the national cybersecurity system in relation to public tasks which depend on information systems and which are performed by that unit's organisational units. Notably, the provision does not stipulate the legal form in which to designate such a contact person (Karpiuk, 2020: 59).

With regard to the responsibility for maintaining contacts with entities within the national cybersecurity system in relation to public tasks which depend on information systems, the legislators have specifically named the local government, while referring to other entities generally as public entities. The local government, as an element of the national cybersecurity system and a public entity responsible for acting for this system, is a local structure which knows the most about matters of concern to the local community (Kostrubiec, 2011: 337). A local government is a legal entity established as separate from the state while also representing the basic form of administrative decentralisation (Karpiuk, 2008: 58). It performs a considerable portion of public tasks delegated by the legislators (Karpiuk, Kostrubiec, 2017: 191; Karpiuk, 2019a: 38), which is why it was given the attribute of control over the performance of public tasks locally (Karpiuk, 2014: 15). One of its obligations is to ensure security in cyberspace (Czuryk, 2019; 40; Czuryk & Kostrubiec, 2019: 34).

Further obligations for public entities are set out by Article 22 of the NCSA , pursuant to which a public entity performing a public task which depends on an information system shall: 1) ensure incident management in that public entity; 2) report any incident in that

public entity immediately, but no later than within 24 hours of its detection, to the responsible CSIRT MON, CSIRT NASK or CSIRT GOV; 3) ensures the handling of any incident in that public entity, or any critical incident, in collaboration with the competent CSIRT MON, CSIRT NASK or CSIRT GOV, by providing the necessary data, including personal data; 4) provides the persons for whom the public task is performed with access to the knowledge required to understand cybersecurity threats and use effective methods of protection against such threats, in particular by publishing related information on its website; 5) provides data on the person in charge of maintaining contacts with entities within the national cybersecurity system, including his/her name and surname, telephone number, and e-mail address, to the competent CSIRT MON, CSIRT NASK or CSIRT GOV, within 14 days of such person being appointed, along with information on changes to such data, within 14 days of such change.

Incident reporting at public entities follows a formal procedure. The elements of this procedure are set out in Article 23 (1) of the NCSA. These include: 1) the details of the reporting entity, including its name, number in the relevant register, head office, and address; 2) name and surname, telephone number and e-mail address of the reporting person; 3) name and surname, telephone number and e-mail address of the person authorised to provide explanations regarding the reported information; 4) a description of the impact of the public-entity incident on a public task, including: a) the public task on which the incident had an impact, b) the number of persons on which the incident had an impact, c) the time at which the incident occurred and was detected, and its duration, d) the geographical range of the incident, e) the cause of the incident, how it unfolded and the consequences of its impact on the information systems of the public entity; 5) information about the cause and source of the incident; 6) information about the preventive measures taken; 7) information about the corrective measures taken; 8) other pertinent information. This information is required to properly identify the threat and, by extension, take appropriate countermeasures. Its purpose is also to facilitate measures to eliminate the threat and its effects, as well as to predict and counteract such a threat in the future.

A public-entity incident is defined in Article 2 (9) of the NCSA as an incident which causes or may compromise the quality, or interrupt the performance, of a public task by a public entity.

Article 23 (3)-(4) of the NCSA stipulates that the public entity's incident report shall include information representing legally protected secrets, including trade secrets, where this is necessary for the competent CSIRT MON, CSIRT NASK or CSIRT GOV to perform its tasks. The competent CSIRT MON, CSIRT NASK or CSIRT GOV may request the public entity which reports the incident to supplement the report with certain information, including information representing legally protected secrets, as required for the performance of the tasks referred to in the Act.

In line with Article 11 (2) of the Unfair Competition Act of 16 April 1993 (consolidated text, (Journal of Laws of 2019, item 1010, as amended), a trade secret is defined as any technical, technological, process-related, organisational or any other information which has inherent economic value and which, whether as a whole or in a specific combination or compilation of its elements, is not commonly known to individuals who typically deal with such information, or which is not easily available to such persons, provided that the individual authorised to use or have such information at his or her disposal has taken measures to keep it confidential.

In its judgement of 8 November 2019, II SA/Wa 1049/19 (LEX No. 2746730) the Provincial Administrative Court described a business secret as comprising two elements: substantive (e.g. a detailed description of how a service will be provided and its cost) and formal (the will to keep certain information a secret). Business secrets constitute information known only to a specific circle of individuals and associated with the company's business in respect of which the company has taken adequate protection measures to keep such information confidential (there is no need for the requirement of economic value to be met, as in the case of a trade secret). Information becomes "a secret" once the company expresses its will to keep such information non-identifiable for third parties. This is supported by the Provincial Administrative Court's judgement of 30 December 2019, II SA/Rz 1266/19 (LEX No. 2825840), which states that in order for a piece of information to be considered "a trade secret", two requirements must be met – a formal and a substantive one. The formal requirement relates to the specific measures taken by the company to keep certain information confidential. Accordingly, it is not sufficient to convince the entity which has information on the company's business at its disposal that such information is confidential. Rather, the company must prove that it has specifically designated such information as confidential. The substantive requirement relates to the contents of such information (technical, technological, process-related, organisational or other information which has inherent economic value for the company) whose disclosure could have an adverse impact on the company's situation. Designating information as confidential alone is insufficient to conclude that an objective situation exists in which such information is a business secret. In order for such undisclosed, confidential and protected information to be actually considered confidential, it must have a technical, technological, process-related organisational or other nature with inherent economic value, as concluded in the Provincial Administrative Court's judgement of 5 December 2019, IV SA/Wr 389/19 (LEX No. 2755728). Finally, it should be stressed that, as stated in the Provincial Administrative Court's judgement of 14 May 2020, VI SA/Wa 2590/19 (LEX No. 3036965), a trade secret, like any statutorily protected secret, is objective in nature, and as such its existence cannot be subjectivised on the mere basis of statements by the company's representatives.

A public entity is required to provide in its incident report information representing legally protected secrets, including classified information, when this is necessary for the competent CSIRT MON, CSIRT NASK or CSIRT GOV to perform its tasks. According

to the definition provided in Article 1 of the Act of 5 August 2010 on the Protection of Classified Information (consolidated text, Journal of Laws of 2019, item 742, as amended – further "the APCI") classified information is information the unauthorised disclosure of which would or could cause harm to the Republic of Poland, or be disadvantageous to its interests, including any disclosure while such information is being developed, regardless of its form and manner of expression. Certain information should be appropriately protected to ensure the state's proper functioning and security. This protection should be guaranteed by providing the information with an appropriate classification designation. By using such a classification – due to circumstances which represent or may represent a threat to state security – the legislators can exclude the principle of transparency in relation to public authorities (Karpiuk, 2018: 85).

As rightly noted by the Provincial Administrative Court in its Judgement of 25 May 2016, IV SA/Wa 3802/15 (LEX No. 2113660), in categorising the types of classified information, the legislators recognise legally protected interests by using qualifiers which allow an assessment in that regard when grading risks in cases involving unauthorised disclosure of information. Consequently, the legislators have established four types of classified information, whose protection depends on the degree of such risks. Legally protected interests which warrant the protection of classified information include security, defence and public order (Czuryk, 2017: 109-110).

Classified information is designated by providing it with an appropriate classification designation. In accordance with Article 5 (1) of the APCI classified information is given the "top secret" classification if its unauthorised disclosure would cause particularly serious harm to the Republic of Poland by: 1) jeopardising the independence, sovereignty or territorial integrity of the Republic of Poland; 2) jeopardising the internal security or constitutional order of the Republic of Poland; 3) jeopardising the alliances or international position of the Republic of Poland; 4) weakening the defence preparedness of the Republic of Poland; 5) causing, or potentially causing, the identification of officers, soldiers or active intelligence or counterintelligence personnel, where such identification may put their operational safety at risk, or lead to the identification of their sources; 6) putting or potentially putting at risk the life or health of officers, soldiers or active intelligence, or counterintelligence personnel, or their sources 7) putting or potentially putting at risk the health or life of crown witnesses, or their closest relatives, and people granted with state protection and assistance available for victims and witnesses, or for anonymous witnesses and their closest relatives. The legislators have introduced classification designations of classified information which depend on the effects the disclosure of such information can have on the state (Karpiuk, Chałubińska-Jentkiewicz, 2015b: 151). Such information is provided with the appropriate classification designation depending on the seriousness of the threat or harm potentially caused by the unauthorised disclosure of this information (Karpiuk, Chałubińska-Jentkiewicz, 2015a: 34). Hence, the appropriate classification designation of classified information is associated with the

threat its unauthorised disclosure can cause (Bożek, Czuryk, Karpiuk & Kostrubiec, 2014: 74).

Classified information is designated as "secret" if its unauthorised disclosure would cause serious harm to the Republic of Poland by: 1) preventing the performance of tasks associated with defending the sovereignty or constitutional order of the Republic of Poland; 2) deteriorating the relations between the Republic of Poland and other states and international organisations; 3) disrupt the state's defence preparations or the functioning of the Armed Forces of the Republic of Poland; 4) hindering intelligence operations conducted to ensure state security and pursue criminals by the authorities and institutions with powers to do so; 5) significantly disrupting the functioning of law enforcement agencies and judicial authorities 6) causing substantial harm to the economic interests of the Republic of Poland – Article 5 (2) of the APCI.

Classified information is designated as "confidential" – under Article 5 (3) of the APCI – if its unauthorised disclosure would cause harm to the Republic of Poland by: 1) hindering foreign policy implementation by the Republic of Poland; 2) hindering the implementation of defence projects, or compromising the combat capability of the Armed Forces of the Republic of Poland; 3) disrupting public order or putting the safety of citizens at risk; 4) obstructing the operations of services and institutions in charge of safeguarding the security or vital interests of the Republic of Poland; 5) obstructing the operations of services and institutions in charge of protecting public order, citizen safety and pursuing criminals, including tax criminals, and of judicial authorities; 6) putting at risk the stability of the financial system of the Republic of Poland; 7) having an adverse impact on the functioning of the national economy.

Classified information is marked as "restricted" where it has not been provided with a higher classification designation and its unauthorised disclosure could adversely affect the tasks of public authorities or other organisational units related to national defence, foreign policy, public security, the protection of civic rights and freedoms, and the economic interests of the Republic of Poland – Article 5 (4) of the APCI. Article 5 (4) of the APCI implies that information openness is excluded for classified information if the disclosure thereof could have an adverse effect on the performance of the above-outlined scope of tasks by the public authorities and other organisational units – this is the line of argumentation offered by the Provincial Administrative Court in its judgement of 15 September 2017, II SA/Kr 1043/17 (LEX No. 2381044). According to the legitimate stance made by the Provincial Administrative Court in its judgement of 9 February 2012, II SA/Wa 2451/11 (LEX No. 1121569), it is clear that entities authorised to designate information as classified should in each case investigate whether an unauthorised disclosure could, from the perspective of the purpose for which classified information is protected, have an adverse effect on the public authorities' or other organisational units' performance of tasks related to national defence, foreign policy, public security,

protection of civic rights and freedoms, the justice system, or the economic interests of the Republic of Poland.

Access to classified information contained in an incident report is not unlimited but granted exclusively to the person which guarantees confidentiality (i.e. fulfils the statutory requirements for the protection of classified information) and only when this is necessary for the competent CSIRT MON, CSIRT NASK or CSIRT GOV to implement its tasks. Classified information may be disclosed only in specific circumstances and to appropriate persons, a fact which proves the special character of such information. Their disclosure is prohibited due to the protection of interests of specific entities defined by law, as well as specific interests set forth by law (Czuryk, 2015; 161). Classified information may be disclosed only when such information is indispensable for taking mandatory action prescribed by law (Chałubińska-Jentkiewicz, Karpiuk, 2015: 443).

It should be stressed that classified information is protected regardless of whether or not the authorised person deemed it appropriate to provide such information with a suitable classification designation. Indeed, information is classified by virtue of the potential threats associated with its contents and not its level of classification, as stated in the Provincial Administrative Court's judgement of 26 October 2015, II SA/Wa 1135/15 (LEX No. 1940909).

A public entity performing a public task which depends on an information system pursuant to Article 24 of the NCSA may provide the competent CSIRT MON, CSIRT NASK or CSIRT GOV with information on 1) other incidents; 2) cybersecurity threats; 3) risk estimation; 4) vulnerabilities; 5) the technologies used. Incidents are reported electronically, and where this is impossible, using other available means of communication.

Pursuant to Article 25 in conjunction with Article 8 of the NCSA the public entity acting as an operator of an essential service is required to implement a security management system in the information system used to provide an essential service in connection with which it has been recognised as an operator of an essential service. Such a security management system is designed to ensure: 1) systematic estimations of the risk of incident occurrence and risk management; 2) the implementation of appropriate technical and organisational measures proportionate to the estimated risk, having regard to the state of the art; 3) the collection of information on cybersecurity threats and vulnerabilities in the information system used for the provision of the essential service; 4) incident management; 5) measures to prevent and mitigate the incident's impact on the security of the information system used for the provision of essential services; 6) the use of means of communications enabling proper and safe communication within the national cybersecurity system.

The public entity acting as an operator of essential services is required to (Article 25 in conjunction with Article 11 (1) of the NCSA): 1) ensure that the incident is handled; 2) provide access to information on the recorded incidents to the competent CSIRT MON, CSIRT NASK or CSIRT GOV, as necessary for the latter to perform its tasks; 3) classify an incident as serious based on serious incident thresholds; 4) notify a serious incident immediately, but not later than within 24 hours of its detection, to the competent CSIRT MON, CSIRT NASK or CSIRT GOV; 5) collaborate in the handling of serious and critical incidents with the competent CSIRT MON, CSIRT NASK or CSIRT GOV by providing the necessary data, including personal data; 6) eliminate vulnerabilities (when coordinating the handling of a serious, substantial or critical incident, CSIRT MON, CSIRT NASK or CSIRT GOV may request the competent authority for cybersecurity to demand that the operator of an essential service eliminate, within a set time limit, the vulnerabilities which led or could have led to a serious, substantial or critical incident) and notifies their elimination to the competent authority for cybersecurity.

The public entity acting as an operator of an essential service in connection with which it has been recognised as such an operator is required to cooperate on the handling of serious and critical incidents. A serious incident is an incident which, pursuant to Article 2 (7) of the NCSA, seriously compromises, or might compromise, the quality of an essential service, or interrupt the continuity of its provision. Under Article 2 (6) of the NCSA a critical incident is an incident which seriously harms security or public order, international interests, economic interests, public institutions' activities, civil rights and freedoms, and/or human health and life, as classified by the competent CSIRT MON, CSIRT NASK or CSIRT GOV.

Among the determinants of a critical incident are security and public order. Security can be described as a multidimensional institution, which makes it elusive, as is the case with other statutorily protected values. Security is seen in the context of the absence of threats. Thus, it can be seen as an institution whose aim is to protect against threats, both internal and external, detect and counteract such threats using its forces and resources, and eliminate the consequences of threats that have already occurred (Karpiuk, 2019c: 5). Security is an institution of great importance for the state as a public institution, as well as for the community and its individual members, and as such it should be treated as the common good (Czuryk, 2018: 15). Security-related tasks must be performed continuously due to the very nature of security (Karpiuk, 2017a: 10). As a social need and a guarantee for the state's functioning, security is a protected value (Karpiuk, 2013: 13).

Public order should be seen through the lens of state order. This order has a public-law dimension and constitutes an organised system of authorities and institutions, or responsibilities, ensuring the stabilisation, alignment, and coordination of measures aimed at neutralising threats (Karpiuk, 2017b: 11). It is an organised system of entities, tools and applicable rules (Karpiuk, 2019c: 169). Public order is determined primarily by the proper arrangement of all its elements such that they form an organised whole to

ensure respect for publicly accepted and legally protected interests. This institution should be founded upon legal standards which are transparent to its addressee (Karpiuk, 2019b: 32).

References

Bosiacki, A. & Kostrubiec, J. (2018) Metropolisation in Poland: current issues and the perspectives, Métropolisation en Pologne: questions actuelles et perspectives, In: Malíková, L., Delaneuville, F., Giba, M. & Guérard, S. (eds.) *Metropolisation, Regionalization and Rural Intermunicipal Cooperation. What impact on Local, Regional and National Governments in Europe? Métropolisation, régionalisation et intercommunalité rurale. Quel impact sur les autorités locales, régionales et centrales en Europe?* (Varenne: Institut Universitaire Varenne), pp. 361-376, pp. 899-914.

Bożek, M., Czuryk, M., Karpiuk, M., Kostrubiec, J. (2014) *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe* (Warszawa: LEX a Wolters Kluwer business).

Chałubińska-Jentkiewicz, K. (2019) Cyberbezpieczeństwo – zagadnienia definicyjne, *Cybersecurity and Law*, 2, pp. 7-23.

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

Czuryk, M. (2019) Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity, *Cybersecurity and Law*, 2, pp. 39-50.

Czuryk, M. (2018) Bezpieczeństwo jako dobro wspólne, *Zeszyty Naukowe KUL*, 3, pp. 15-24.

Czuryk, M. & Kostrubiec, J. (2019) The legal status of local self-government in the field of public security, *Studia nad Autorytaryzmem i Totalitaryzmem*, 41(1), pp. 33-47, https://doi.org/10.19195/2300-7249.41.1.3.

Czuryk, M. (2015) *Informacja w administracji publicznej. Zarys problematyki* (Warsaw: Elpil).

Czuryk, M. (2017) *Właściwość Rady Ministrów oraz Prezesa Rady Ministrów w zakresie obronności, bezpieczeństwa i porządku publicznego* (Olsztyn: the University of Warmia and Mazury in Olsztyn).

Karpiuk, M. (2017a) Konstytucyjna właściwość Sejmu w zakresie bezpieczeństwa państwa, *Studia Iuridica Lublinensia*, 4, pp. 9-24, http://dx.doi.org/10.17951/sil.2017.26.4.9.

Karpiuk, M. (2017b) Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny, *Przegląd Prawa Wyznaniowego*, 9, pp. 5-20.

Karpiuk, M. (2018) Miejsce bezpieczeństwa osobowego w systemie ochrony informacji niejawnych, *Studia nad Autorytaryzmem i Totalitaryzmem*, 1, pp. 85-99.

Karpiuk, M. (2019a), Activities of the local government units in the scope of telecommunication, *Cybersecurity and Law*, 1, pp. 37-48.

Karpiuk, M. (2019b) Position of the Local Government of Commune Level in the Space of Security and Public Order, *Studia Iuridica Lublinensia*, 2, pp. 27-39, http://dx.doi.org/10.17951/sil.2019.28.2.27-39.

Karpiuk, M. (2019c) The legal grounds for revoking weapons licences, *Cybersecurity and Law*, 2, pp. 165-174

Karpiuk, M. (2020) The obligations of public entities within the national cybersecurity system, *Cybersecurity and Law*, 2, pp. 57-72.

Karpiuk M. (2014) *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego* (Warsaw: the National Defence University of Warsaw).

Karpiuk M. (2013) *Zadania i kompetencje zespolonej administracji rządowej w sferze bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty materialne i formalne* (Warsaw: the National Defence University of Warsaw).

Karpiuk, M. (2008) *Samorząd terytorialny a państwo. Prawne instrumenty nadzoru nad samorządem gminnym* (Lublin: the John Paul II Catholic University of Lublin).

Karpiuk, M., Chałubińska-Jentkiewicz, K. (2015a) *Informacja i informatyzacja w administracji publicznej* (Warsaw: the National Defence University of Warsaw).

Karpiuk, M., Chałubińska-Jentkiewicz, K. (2015b) *Prawo bezpieczeństwa informacyjnego* (Warsaw: the National Defence University of Warsaw).

Karpiuk M., Kostrubiec J. (2017) *Rechtsstatus der territorialen Selbstverwaltung in Polen* (Olsztyn: the University of Warmia and Mazury in Olsztyn).

Karpiuk, M. (2014) Cyfrowe transmisje radiofoniczne i telewizyjne i ich wpływ na bezpieczeństwo informacyjne, In: Oleksiewicz, I., Polinceusz, M., Pomykała, M. (eds.), *Nowoczesne technologie – źródło zagrożeń i narzędzie ochrony bezpieczeństwa* (Rzeszów: Oficyna Wydawnicza Politechniki Rzeszowskiej), pp. 33-42.

Kostrubiec, J. (2011) Źródła prawa, In: Dubel, L., Kostrubiec, J., Ławnikowicz, G. & Markwart, Z., *Elementy nauki o państwie i polityce* (Warsaw: Wolters Kluwer), pp. 326-342.

Kostrubiec, J. (2020) Building Competences for Inter-Municipal and Cross-Sectoral Cooperation as Tools of Local and Regional Development in Poland. Current Issues and Perspectives, In: Hințea, C., Radu, B. & Suciu, R. (eds.) *Collaborative Governance, Trust Building and Community Development*. *Conference Proceedings 'Transylvanian International Conference in Public Administration', October 24-26, 2019, Cluj-Napoca, Romania* (Cluj-Napoca: Accent), pp. 186-201, available at: https://www.apubb.ro/intconf/wp-content/uploads/2020/08/TICPA_Proceedings_2019.pdf (November 8, 2020).