The Tasks of Public Entities within the National Cybersecurity System

MIROSŁAW KARPIUK

Abstract The national cybersecurity system is based on public entities, for which the legislators have set the objective of ensuring cybersecurity at the national level, including the undisrupted provision of essential services and digital services by attaining a sufficiently high level of security of information systems serving the purpose of providing such services, and by ensuring incident handling. Public entities perform vital tasks as part of the national cybersecurity system, which involve counteracting disruptions in the functioning of cyberspace. The efficiency of the system warrants the proper operation of the state and local government authorities as well as of public entities operating within their structures, the security of business transactions (including in strategic sectors) and the security of the society. The development of information systems – perceived as information and communications technology systems, which is a set of interfacing IT hardware and software, providing the facility to process, store, send, and receive data via ICT networks, with the use of an end device suitable for a given network type, together with the data processed electronically within the system – facilitates a faster access to information, improved management and economic growth, and makes society increasingly affluent. The increased responsibility for cybersecurity should be proportional to the development rate of information systems, and thus appropriate security systems should be developed with a view to providing safeguards against the unlawful disruption of activity in cyberspace. Protective measures in this respect are part of the obligations entrusted to public entities. This chapter describes the tasks performed by CSIRT MON, CSIRT NASK and CSIRT GOV, the minister competent for computerisation and the Minister of National Defence. It does not include the tasks of all entities within the national cybersecurity system, but the functions of selected entities.

Keywords: • cybersecurity • public entity • incident • martial law • Minister of National Defence

CORRESPONDENCE ADDRESS: Mirosław Karpiuk, PhD., Dr. Habil., Full Professor, University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, Department of Administrative Law and Security Sciences, ul. Obitza 1, 10-725 Olsztyn, Poland, email: miroslaw.karpiuk@uwm.edu.pl.

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

1 The tasks of CSIRT MON, CSIRT NASK and CSIRT GOV

The tasks of public entities, including CSIRT MON, CSIRT NASK and CSIRT GOV, are defined in the National Cybersecurity System Act of 5 July 2018 (consolidated text, Polish Journal of Laws of 2020, item 1396, as amended) – "the NCSA". The entities were defined in Article 2 (1)-(3) of the NCSA, under which 1) CSIRT MON is a Computer Security Incident Response Team operating at the national level, managed by the Minister of National Defence, 2) CSIRT NASK is a Computer Security Incident Response Team operating at the national level, managed by the Research and Academic Computer Network – the National Research Institute, and 3) CSIRT GOV is a Computer Security Incident Response Team operating at the national level, managed by the Head of the Internal Security Agency.

CSIRT MON is managed by the Minister of National Defence who is in charge of the government administration department of national defence, and the authority through which the President of the Republic of Poland has command over the Polish Armed Forces in peacetime. In peacetime, the Minister of National Defence manages the operations of Branches of the Armed Forces with the support from the Chief of the General Staff of the Polish Armed Forces, and the Commander of the Territorial Defence Forces, until the Territorial Defence Forces reach its full operational capacity – Articles 1(1) and 6 of the Act on the Authority of the Minister of National Defence of 14 December 1995 (consolidated text, Polish Journal of Laws of 2019, item 196).

CSIRT NASK is managed by the Research and Academic Computer Network – the National Research Institute. Under § 1 of the Regulation of the Council of Ministers of 7 June 2017 on granting the status of a national research institute to the Research and Academic Computer Network (Polish Journal of Laws of 2017, item 1193, as amended), "NASK Regulation", the Research and Academic Computer Network is awarded the status of a national research institute. A research institute is a state organisational unit, separate in legal, organisational and financial terms, which conducts scientific research and development work aimed at their implementation and practical application – Article 1 (1) of the Act of 30 April on Research Institutes (consolidated text, Polish Journal of Laws of 2020, item 1383, as amended). Pursuant to § 2 of the NASK Regulation, the objects of NASK's activities include: 1) conducting research & development work in: a) telecommunications, b) communication and information technology, c) information technology, d) cybersecurity, e) functioning of the Polish domain name registry, f) information society, 2) adapting the results of research and development work to their practical application; 3) implementing the results of research and development work in services provided for the purposes of, i.a., authorities responsible for public safety and order, state security and the security of critical infrastructure units.

CSIRT GOV is managed by the Head of the Internal Security Agency ("the ISA") who is a central government authority, acting with the support from the ISA, being a government administration agency. The Head of ISA reports directly to the Prime Minister, and ISA

operations are subject to Parliament oversight – Article 3 of the Act of 24 May 2002 on the Internal Security Agency and on the Intelligence Service (consolidated text, Polish Journal of Laws of 2020, item 27).

Under Article 26(2) of the NCSA, the legislators expressly stated that, in justified cases, CSIRT MON, CSIRT NASK and CSIRT GOV may provide support in incident handling at the request of operators of essential services, digital service providers, public entities, sectoral cybersecurity teams or owners, owner-like possessors, or holders of facilities, installations, devices, and services which comprise critical infrastructure. Activities facilitating the detection, registration, analysis, classification, taking corrective measures and mitigation of incident impact require significant involvement. In the event of a major threat to cyberspace, it is possible that public entities obligated to ensure incident handling will not be able to fulfil this task, which constitutes grounds for requesting for support from CSIRT MON, CSIRT NASK and CSIRT GOV, which may be provided in justified circumstances. Assistance may be provided, for example, in the event of threats affecting critical infrastructure. A uniform list of facilities, installations, devices, and services which comprise critical infrastructure, divided by systems, which might be a target of an attack and requires support from CSIRT MON, CSIRT NASK and CSIRT GOV, is compiled, pursuant to Article 5b (7) (1) of the Act of 26 April 2007 on Crisis Management (consolidated text, Polish Journal of Laws of 2019, item 1398, as amended – "the CMA"), by the Director of the Government Centre for Security in collaboration with relevant ministers in charge of the systems.

The catalogue of tasks entrusted to CSIRT MON, CSIRT NASK and CSIRT GOV was defined in Article 26 (3) of the NCSA, and includes: 1) monitoring cybersecurity threats and incidents at national level; 2) estimating risks related to the identified threat and incidents, including the performance of dynamic risk analysis; 3) providing information concerning incidents and risks to other entities within the national cybersecurity system; 4) issuing alerts on identified cybersecurity threats; 5) responding to notified incidents, 6) classifying incidents, including serious and significant incidents, as critical incidents, and coordinating the process of critical incident handling; 7) reclassifying serious and significant incidents; 8) providing the relevant CSIRT MON, CSIRT NASK or CSIRT GOV with technical information on incidents, the handling of which needs to be coordinated by way of collaboration between CSIRTs, 9) inspecting, in justified cases, IT equipment or software with the aim of identifying any vulnerability which, when used, can threaten, in particular, the integrity, confidentiality, accountability, authenticity or availability of processed data, and affect public security or the material interest of the state security, as well as submitting applications regarding recommendations for entities within the national cybersecurity system on the use of IT equipment and software, especially as regards their impact on public security or the material interest of the state security, 10) cooperating with sectoral cybersecurity teams in the field of coordination of serious incident handling, including incidents concerning two or more EU Member States, and critical incidents, as well as the exchange of information enabling the counteracting of threats to cybersecurity; 11) providing to, and receiving from, other

countries, including EU Member States, information on serious and significant incidents concerning two or more EU Member States, and submitting to the Single Point of Contact notifications of serious and significant incidents concerning two or more EU Member States; 12) providing, by 30 May each year, to the Single Point of Contact a list of serious incidents notified in the preceding calendar year by operators of essential services, which had affected the continuity of their provision of essential services in the Republic of Poland, and their provision of essential services in EU Member States, as well as a list of significant incidents notified in the preceding calendar year by digital service providers, including those concerning two or more EU Member States; 13) jointly compiling and providing to the minister competent for computerisation the part of the Report on threats to national security regarding cybersecurity; in accordance with Article 5a (1)-(2) of the CMA, for the purpose of the National Crisis Management Plan, the ministers in charge of government administration departments, heads of central agencies and province governors (Kostrubiec, 2018:36) prepare a Report on Threats to National Security. The Director of the Government Centre for Security coordinates work on such a report, which is also a task entrusted to the Head of the Internal Security Agency in a part concerning terrorist threats which can result in a crisis situation, and to the Government Plenipotentiary for Cybersecurity in the part comprising cybersecurity threats which could result in a crisis situation; 14) ensuring analytical and R&D infrastructure, intended for, in particular, a) conducting advanced malware analyses and vulnerability analyses, b) monitoring cybersecurity threat indicators, c) developing tools and methods for detecting and combating cybersecurity threats, d) conducting analyses and developing standards, recommendations and good practices as regards cybersecurity, e) supporting entities within the national cybersecurity system in capacity building in the sphere of cybersecurity, f) conducting awareness raising activities in the sphere of cybersecurity, g) cooperating in the scope of educational solutions in relation to cybersecurity; 15) ensuring the possibility of submitting notifications and providing information, as well as providing access to and operating means of communication allowing such notifications to be submitted; 16) participating in the CSIRT network comprising representatives of the CSIRTs in EU Member States, the CSIRT responsible for the institutions of the European Union, the European Commission and the European Union Agency for Network and Information Security (ENISA).

Under Article 26 (5) of the NCSA, CSIRT MON is responsible for coordinating the handling of incidents notified by 1) entities subordinate to, or supervised by, the Minister of National Defence, including entities whose information and communication systems or networks are included in the uniform list of facilities, installations, devices, and services which comprise critical infrastructure; 2) 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 (see also Article 5 (3) of the Act of 23 August 2001 on the Organisation of Tasks for State Defence Performed by Enterprises (Polish Journal of Laws No. 122, item 1320, as amended). CSIRT MON is an entity which coordinates the handling of incidents reported by relevant entities. The notion of coordination specifies a set of powers exercised by an appropriate

authority in relation to entities which are nor directly subordinated to such authority. These are units subordinate to other authorities, or entities operating independently. Coordination in public administration entails the harmonisation of the activities performed by various public authorities and agencies with a view to pursuing specific objectives (Szczęch, 2013: 21).

Under Article 26 (6) of the NCSA, CSIRT NASK is responsible for: 1) coordinating the handling of incidents notified by entities specified in the NCSA, 2) creating and providing tools for voluntary cooperation, and the exchange of information on cybersecurity threats and incidents, 3) providing a telephone or Internet service for reporting and analysing instances of distribution, dissemination, or transmission of child pornography through information and communication technologies. Child pornography' means: a) any material that visually depicts a child engaged in real or simulated sexually explicit conduct; b) any depiction of the sexual organs of a child for primarily sexual purposes; c) any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes; or d) realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes – Article 2 (c) of Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (Official Journal EU L 335, p. 1) (Radoniewicz, 2019).

The tasks of CSIRT GOV, as laid down in Article 26 (7) of the NCSA, include the coordination of handling incidents notified by: 1) public authorities, including government administration authorities, state control and legal protection authorities, and courts and tribunals; 2) the Social Insurance Institution and funds managed by it, the Agricultural Social Insurance Fund and funds managed by the President of the Agricultural Social Insurance Fund; 3) the National Health Fund; 4) entities subordinate to or supervised by the Prime Minister; 5) the National Bank of Poland, 6) the National Economy Bank, 7) other entities whose information and communication systems or networks are included in the uniform list of facilities, installations, devices, and services which comprise critical infrastructure.

CSIRT GOV is a competent authority for incidents related to terrorist events, which should be understood as a situation which is suspected to have arisen from an offence of a terrorist nature, as stipulated in Article 2 (7) of the Act of 10 June 2016 on Anti-Terrorism (consolidated text, Polish Journal of Laws of 2019, item 796). An offence of a terrorist nature is a prohibited act punishable by imprisonment with a maximum term of at least five years, committed with the aim of: 1) seriously intimidating a large number of people, 2) compelling a public authority of the Republic of Poland or another state or an authority of an international organisation to undertake or refrain from undertaking any specific act, 3) causing any serious disruption to the political system or the economy of the Republic of Poland or another state or international organisation, and also a threat of

committing any such act. The definition of a terrorist offence is laid down in Article 115 § 20 of the Act of 6 June 1997 – the Penal Code (consolidated text, Polish Journal of Laws of 2020, item 1444, as amended). The competence of CSIRT GOV with regard to incidents related to terrorist events arises from the provisions set out in Article 27 (1) of the NCSA (Radoniewicz, 2019).

In accordance with Article 27 (2) of the NCSA, CSIRT MON is a competent authority in the scope of incidents related to terrorist events which undermine the security of the defence potential of the state, the Polish Armed Forces, and the organisational units of the Ministry of National Defence.

2 The tasks of the minister competent for computerisation

The minister competent for computerisation manages the government administration department of computerisation which comprises the following: 1) computerisation of public administration and entities performing public tasks; 2) information and communication systems and networks of public administration, 3) support for computerisation projects, 4) fulfilment of international commitments of the Republic of Poland in respect of computerisation and telecommunications; 5) participation in developing the computerisation policy of the European Union; 6) development of information society and counteracting digital exclusion; 7) development of services provided by electronic means; 8) development of the state policy on personal data protection; 9) telecommunications; 10) the civil aspect of cyberspace security; 11) the PESEL register, Register of Identity Cards, Civil Registry, and the Central Register of Issued and Cancelled Passport Documents; 12) the vehicle register, drivers' register, and parking-card holders' register; 13) the supervision over the provision of trust services within the meaning of trust-services regulations; 14) and electronic identification. The minister competent for computerisation exercises supervision over the President of the Office of Electronic Communications. The above competence arises from Article 12a of the Act of 4 September 1997 on Government Administration Departments (consolidated text, Polish Journal of Laws of 2020, item 1220, as amended), "AGAD."

As stipulated in Article 45 of the NSCA, the minister competent for computerisation is responsible for: 1) monitoring the implementation of the Cybersecurity Strategy of the Republic of Poland, and associated action plans; 2) recommending the spheres of cooperation with the private sector in order to increase the cybersecurity of the Republic of Poland; 3) preparing annual reports regarding: a) serious incidents notified by operators of essential services affecting the continuity of provision of their essential services in the Republic of Poland and in the Member States of the European Union; b) significant incidents notified by digital service providers, including those involving two or more European Union Member States; 4) conducting informational activities on good practices, educational programmes, campaigns, and training, to expand knowledge and build awareness of cybersecurity, including the safe use of the Internet by various categories of users; 5) collecting information on serious incidents which concerns, or has been provided

by, another Member State of the European Union; 6) providing information and good practices related to the notification of serious incidents by operators of essential services, and significant incidents by digital service providers, obtained from the Cooperation Group, including a) incident-management procedures, b) risk-management procedures, c) and the classification of information, risks, and incidents. The Cooperation Group was established to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence, and with a view to achieving a high common level of security of network and information systems in the Union – Article 11 (1) of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (Official Journal EU L 194, p. 1). The Cooperation Group is chaired by a representative of the Member State holding the Presidency in the Council of the European Union The Chair is assisted in the performance of his duties by representatives of the Member States holding the previous and the following Presidency of the Council of the European Union – Article 2 (1) of Commission implementing Decision (EU) 2017/179 of 1 February 2017 laying down procedural arrangements necessary for the functioning of the Cooperation Group pursuant to Article 11(5) of the Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (Official Journal EU L 28, p. 73).

An important task entrusted to the minister competent for computerisation is to run the Single Point of Contact with competencies including, under Article 48 of the NCSA, 1) receiving notifications of serious or significant incidents involving two or more European Union Member States from single points of contact in other EU Member States and forwarding such notifications to CSIRT MON, CSIRT NASK, CSIRT GOV or sectoral cybersecurity teams, 2) forwarding, at the request of a relevant CSIRT MON, CSIRT NASK, or CSIRT GOV notifications of serious or significant incidents involving two or more EU Member States to single points of contact in other EU Member States; 3) ensuring the representation of the Republic of Poland in the Cooperation Group, 4) ensuring cooperation with the European Commission in the sphere of cybersecurity, 5) coordinating cooperation between competent authorities for cybersecurity and public authorities in Poland with relevant authorities in other EU Member States; 6) ensuring the exchange of information for the benefit of the Cooperation Group, and the CSIRT Network. The Single Point of Contact plays a significant function with regard to cybersecurity cooperation at the European Union level.

3 The tasks of the Minister of National Defence

The Minister of National Defence manages the government administration department of national defence, which, under Article 19 of the GADA, includes the following matters in peacetime, 1) state defence and Armed Forces of the Republic of Poland; 2) the military aspect of cyberspace security; 3) the participation of the Republic of Poland in the military projects of international organisations, and fulfilling the military tasks arising

from international agreements and 4) offset arrangements, unless, under separate legal regulations, specific matters belong to the obligations and competences of the President of the Republic of Poland or other state authorities.

Pursuant to Article 51 of the NCSA, the Minister of National Defence is responsible for: 1) ensuring the cooperation of the Armed Forces of the Republic of Poland with the relevant authorities of the North Atlantic Treaty Organisation, the European Union and other international organisations, in the field of national defence and, more specifically, cybersecurity; 2) ensuring the capacities of the Armed Forces of the Republic of Poland, in the domestic, alliance and coalition relations, for conducting military operations in the event of a threat to cybersecurity triggering the need to take defensive measures; 3) developing the abilities of the Armed Forces of the Republic of Poland as regards the provision of cybersecurity by organising specialised training; 4) acquiring and developing tools to be used by the Armed Forces of the Republic of Poland for capacity-building as regards the provision of cybersecurity; 5) managing activities related to incident handling under martial law; 6) assessing the impact of incidents on the state's defence system; 7) assessing threats to cybersecurity under martial law and presenting proposals regarding defensive measures to competent bodies; 8) coordinating, in cooperation with the minister competent for internal affairs and the minister competent for computerisation, the performance of duties by government administration and local government authorities under martial law, regarding defensive measures in the event of a threat to cybersecurity.

The obligations entrusted to the Minister of National Defence under martial law in the event of appointing the Commander-in-Chief of the Army might arise certain doubts. The duality of powers under martial law can be observed here, as two (possibly conflicting) decision-making centres operate during such time, which is detrimental to the implementation of the state defence policy and the military operations themselves. Combatting external threats to the state resulting from actions in the cyberspace might prove ineffective or extended in time in the event of conflicting positions of the Minister of National Defence and Commander-in-Chief of the Army, which can be detrimental to the state.

During wartime, the President of the Republic of Poland, at the request of the Prime Minister, may appoint the Commander-in-Chief of the Army (Karpiuk, 2015: 5). The President does not act independently in this respect, but in collaboration with government administration (Karpiuk, 2013: 201). Having command over the Polish Armed Forces, as a rule, the President of the Republic of Poland does not have the power to act independently, although this is a case of "the highest command." The President exercises his powers based on the principle of collaboration (Karpiuk, 2019: 21).

In the event of an external threat to the state, including terrorist acts or activities in the cyberspace, an armed aggression on the territory of the Republic of Poland, or an obligation of joint defence against aggression arises from international commitments, the President of the Republic of Poland may, at the request of the Council of Ministers,

introduce martial law across a part or whole of the state territory. The procedure was introduced under Article 2 (1) of the Act of 29 August 2002 on the Martial Law and the Competences of the Commander-in-Chief of the Army and the Rules of the Commander-in-Chief's Subordination to the Constitutional Authorities of the Republic of Poland (consolidated text, Polish Journal of Laws of 2017, item 1932, as amended, the "MLA"). The objective of the martial law is to counteract threats which affect the functioning of the state (Czuryk, 2013: 75). Operations in the cyberspace, being a space for the processing and exchange of information created by information and communication systems, including the links between them and their relations with users, might constitute grounds for the introduction of martial law.

Not every threat can result in introducing a state of emergency, only threats of special importance, with a substantial degree of intensity and interference, which public authorities are unable to address using standard tools and procedures (Karpiuk, 2017: 98). Cybersecurity threat might be a premise to introduce martial law, as a state of emergency, provided that it is aggravated, and therefore standard constitutional measures have proven insufficient to counteract such threat.

Under Article 16 of the MLA, the Commander-in-Chief of the Army has command over the Armed Forces of the Republic of Poland and other organisational units subordinated to the Commander-in Chief in line with the national plans for the deployment of the Armed Forces for state defence purposes. In particular, the Commander-in-Chief of the Army: 1) has command over the Armed Forces of the Republic of Poland in order to repulse armed aggression on the territory of the Republic of Poland, 2) ensures cooperation of the subordinate Armed Forces of the Republic of Poland with allied forces in planning and conducting military operations, 3) defines, within his competences, the needs of the Armed Forces of the Republic of Poland in the scope of support from the non-military part of the state defence system; 4) appoints military authorities to perform the tasks of government and local government administration in the combat zone, and defines their tasks and powers (Kostrubiec, 2021: 115-118). It is the Commander-in-Chief of the Army that is the manager, coordinator and organiser of defence operations during the martial law, and therefore, in the event of a cybersecurity threat the Commander-in-Chief, not the Minister of National Defence, should make strategic decisions, and the minister should play a support function.

Under Article 52 of the NCSA, the Minister of National Defence runs the National Point of Contact for Cooperation with NATO, responsible for: 1) ensuring cooperation in the sphere of national defence with competent NATO authorities as regards cybersecurity; 2) coordinating defence capacity building measures in the event of cybersecurity threat; 3) ensuring cooperation between national and allied armed forces in the sphere of cybersecurity; 4) developing systems of information exchange concerning cybersecurity threats in the national defence domain; 5) participating in the fulfilment of NATO objectives in the sphere of cybersecurity and cryptology.

References:

Czuryk, M. (2013) Podstawy prawne bezpieczeństwa narodowego w stanie kryzysu i wojny, *Roczniki Nauk Społecznych*, 3, pp. 69-92.

Karpiuk, M. (2015) Normatywne uwarunkowania stanu wojennego i wyjątkowego, *Studia Prawnicze i Administracyjne*, 3, pp. 3-9.

Karpiuk, M. (2013) *Kształtowanie się instytucji stanów nadzwyczajnych w Polsce* (Warsaw: WSM).

Karpiuk, M. (2019) *Służba wojskowa żołnierzy zawodowych* (Olsztyn: UWM).

Karpiuk, M. (2017) Zadania i kompetencje samorządu terytorialnego w czasie stanów nadzwyczajnych, In: Karpiuk, M., Mazuryk , M. & Wieczorek I. (eds) *Zadania i kompetencje samorządu terytorialnego w zakresie porządku publicznego i bezpieczeństwa obywateli, obronności oraz ochrony przeciwpożarowej i przeciwpowodziowej*, (Łódź: NIST), pp. 98-104.

Kostrubiec, J. (2021) The Role of Public Order Regulations as Acts of Local Law in the Performance of Tasks in the Field of Public Security by Local Self-government in Poland, *Lex Localis - Journal of Local Self-Government*, 19(1), pp. 111-129, https://doi.org/10.4335/19.1.111-129(2021).

Kostrubiec, J. (2018) Status of a Voivodship Governor as an Authority Responsible for the Matters of Security and Public Order, *Barometr Regionalny. Analizy i Prognozy*, 16(5), pp. 35-42, available at: http://br.wszia.edu.pl/zeszyty/pdfs/br54a_04kostrubiec.pdf (March 15, 2020).

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

Szczęch, N. (2013) Administracja publiczna i prawo administracyjne, In: Karpiuk, M. & Kowalski, J. (eds.) *Administracja publiczna i prawo administracyjne w zarysie* (Warszawa-Poznań: Iuris), pp. 15-28.