The Competence of the Internal Security Agency in Protecting the Security of Communication and Information Systems and Networks of Public Administration Authorities

MIROSŁAW KARPIUK

Abstract The Internal Security Agency (ISA), which is one of Poland's special services, has competence over matters entailing the protection of the state's internal security and its constitutional order. Its tasks include the identification, prevention and combating of threats to the internal security of the state and its constitutional order, in particular those affecting the sovereignty and international status of the state, its independence and inviolability of state borders, as well as the state defence capabilities. The ISA is also obligated to protect the security of communication and information systems of public administration authorities that are significant for the continuity of state functioning, and/or the system of ICT networks which are included in the uniform list of facilities, installations, devices and services which comprise critical infrastructure. Cyberspace is one of the areas of operations pursued by this civil intelligence service, where its task is to protect communication and information systems of primary significance to the functioning of public administration within the framework of state structures.

Keywords: • special services • cybersecurity • communication and information systems • ICT networks • public administration

CORRESPONDENCE ADDRESS: Mirosław Karpiuk, PhD., Prof. 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, e-mail: miroslaw.karpiuk@uwm.edu.pl, ORCID: 0000-0001-7012-8999.

https://doi.org/10.4335/2022.1.7 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

Communication and information systems and networks are exposed to cyber-attacks, so the telecommunications infrastructure should be continuously protected in order to prevent such threats. The Internal Security Agency (ISA) has the obligation to provide such protection. The competence of the ISA in respect of identifying, preventing and combating threats to the security of communication and information systems of public administration authorities is falls within the domain of cybersecurity. The tasks of this special service include the provision of security in cyberspace. Cyberspace is understood as a space for the processing and exchange of information, comprised of communication and information systems, including the links between them and their relations with users (Chałubińska-Jentkiewicz, Karpiuk, Kostrubiec, 2021: 1).

The challenges posed by the new digital era have compelled public administration authorities to introduce changes (Hoffman, Cseh, 2020: 210). Contemporary public administration acts on the basis of communication and information systems and networks that need to be properly protected against cyber-attacks. The role of the state is to ensure cybersecurity within public institutions. The National Cybersecurity System Act of 5 July 2018 (consolidated text, Polish Journal of Laws of 2020, item 1369, as amended), as per Article 2(4), defines cybersecurity as the resilience of information systems against operations that compromise the availability, authenticity, integrity and confidentiality of processed data, or the related services offered by those information systems. Cybersecurity constitutes a specialised security system component that covers the protection of information systems against threats (Czuryk, 2019: 42).

2 The competence of the Internal Security Agency in cybersecurity

The Internal Security Agency (ISA) is a civil special service which has, like other special forces, competence over security affairs (Bożek, Czuryk, Karpiuk, Kostrubiec, 2014: 43). It was established to protect the internal security of the state and its constitutional order. This competence arises from the provisions of Article 1 of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency (consolidated text, Polish Journal of Laws of 2020, item 27, as amended) – further referred to as "the AISA". This general competence of the ISA also encompasses the provision of cybersecurity in public administration through the protection of communication and information systems and networks operated by public administration. The statutory responsibilities of the ISA include the identification, prevention and investigation of threats to the security of communication and information systems of public administration authorities that are significant for the continuity of state functioning, and/or ICT networks that are included in the uniform list of facilities, installations, devices and services which comprise critical infrastructure, as well as the communication and information systems belonging to the owners or holders of critical infrastructure facilities, installations and devices, as

expressly laid down in Article 5(1)(2a) of the AISA. In line with the definition set out in Article 2(3) 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, as amended), a communication and information system is a set of cooperating IT hardware and software providing the capability to process and store, as well as send and receive, data via ICT networks with the use of telecommunications terminal equipment suitable for a given network type. Under Article 2(43) of the Telecommunications Law of 16 July 2004 (consolidated text, Polish Journal of Laws of 2021, item 576, as amended) telecommunications terminal equipment is understood as telecommunications devices intended for direct or indirect connection with network termination points. An ICT network includes software operated by the devices that have access to it, allowing users to browse, create, disseminate and exchange data and information (digital content) as part of network access (Chałubińska-Jentkiewicz, 2019: 132). Critical infrastructure is understood as systems and functionally linked facilities forming part of the systems, including buildings, devices, installations, essential services of key importance to the security of the state and its citizens, and services intended to provide efficient operations of public administration authorities, institutions and enterprises - Article 3(2) of the Crisis Management Act of 26 April 2007 (consolidated text, Polish Journal of Laws of 2020, item 1856, as amended), hereinafter "the CMA".

3 The assessment of the security of communication and information systems of public administration authorities that are significant for the continuity of state functioning

Due to the need to ensure cybersecurity in public administration, as per Article 32a(1) of the AISA, the ISA is obliged to assess the security of communication and information systems and networks. This is undertaken with a view to preventing, counteracting and combating terrorist incidents that may affect the communication and information systems of public administration authorities that are significant for the continuity of state functioning, and/or ICT networks which are included in the uniform list of facilities, installations, devices, and services that comprise critical infrastructure, as well as the communication and information systems belonging to the owners, owner-like possessors or lessees of critical infrastructure facilities, installations and devices, or of the data processed in the said systems. The ISA is also compelled to prevent and investigate terrorist offences affecting this sphere, and to prosecute the perpetrators of such offences. To these ends, the ISA may assess the security of these communication and information systems. This last is not an obligation on the part of this special service, but a power that it should, nonetheless, exercise where a terrorist threat occurs. As stipulated in Article 5b(7)(1) of the CMA, the Head of the Government Centre for Security, in collaboration with competent ministers, prepares a uniform list of facilities, installations, devices and services which comprise critical infrastructure, divided by systems, and classified. It also includes European critical infrastructure located on the territory of the Republic of

Poland, and European critical infrastructure located on the territories of other EU Member States that might have a significant impact on Poland. The list is classified.

The objectives of the assessment of communication and information systems of public administration authorities are to prevent, counteract and combat terrorist incidents, and to prevent and investigate terrorist offences affecting this sphere, and prosecute their perpetrators. Under Article 2(7) of the Act of 10 June 2016 on Counter-Terrorism Measures (consolidated text, Polish Journal of Laws of 2019, item 796, as amended) a terrorist incident is understood as a situation where there is a suspicion that such incident has occurred as a result of a terrorist offence, or where a threat of such offence has been identified. In turn, a terrorist offence is a prohibited act subject to imprisonment with the upper sentence limit of at least 5 years, committed with the aim of seriously intimidating a population, unduly compelling a public authority of the Republic of Poland or another state Government or international organisation to perform or abstain from performing an act, or seriously destabilising or destroying the structures or the economy of the Republic of Poland, another state or an international organisation, or a threat of committing such act, as stipulated 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), hereinafter "the PC".

Pursuant to Article 32a(2) of the AISA, the assessment of the security of communication information systems and networks is performed in line with the annual security assessment plan, prepared by 30 September in the preceding year by the Head of ISA, in consultation with the minister in charge of computerisation. Where justifiable, the security assessment may be performed even if it has not been included in the plan. Planning, including with regard to cyberspace, facilitates coordinated measures allowing a proper, timely and balanced performance of tasks assigned to public administration in a well-organised and uninterrupted manner (Karpiuk, 2021: 46). As a rule, the annual plan is the basis for performing the assessment of the security of communication and information systems. The plan is the outcome of cooperation between the Head of ISA (as a central government administration body) and the minister in charge of computerisation (responsible for managing an administration department which entails matters related to communication and information systems and networks of public administration). The cooperation assumes a specific form, i.e., consultation.

The ISA informs the entity managing a given communication and information system that the system is to be included in the annual security assessment plan. This information obligation is imposed under Article 32a(3) of the AISA. The information concerning the date and range of security tests to be performed allows a proper preparation for assessment, including certain restrictions on the performance of public tasks by the administration body whose communication and information system is to be tested.

As per § 4(1) of the Regulation of the Council of Ministers of 19 July 2016 on the performance of security assessment in relation to preventing terrorist incidents (Polish Journal of Laws of 2016, item 1076), hereinafter "the SAR", prior to security assessment, the ISA requests the entity which manages the system concerned to provide information about the system, which may include: 1) system architecture (system architecture is a description of the components of a communication and information system or an ICT network, and their links and relationships to each other), including information on the hardware forming part of the system infrastructure; 2) IP addressing of the system's network infrastructure; 3) information on the current backup copy and the rules of its update, 4) definition of the required system recovery time based on the backup copy; 5) information on the test environment and its range, 6) ICT security features, 7) system security procedures, 8) details of the person appointed by the system managing entity to contact the ISA during the security assessment on an ongoing basis, and 9) details of the person authorised to represent the system managing entity. Given the objective to be achieved by the assessment of the security of communication and information systems of public administration authorities, i.e. counteracting terrorism, the information requested by the ISA should be provided. The information about communication and information systems disclosed to the ISA allow it to perform a full security assessment.

Pursuant to Article 32a(4) of the AISA, security assessment involves security tests on a communication and information system with a view to identifying vulnerabilities, understood as weak points of resources or a security features in a communication and information system which may be used by a threat source and affect the integrity, confidentiality, accountability, and accessibility of the system. Improper security of a communication and information system of a public administration authority might result in its disrupted operations. Cyberthreats can lead to disruptions in the functioning of public institutions, which directly affects their security.

Security assessments are performed in line with the minimisation principle. Pursuant to the provisions of Article 32a(5) of the AISA, the ISA should perform the assessment subject to the principle of minimising the interruptions in system operations, or its restricted availability, and may not result in irreparable damage to data processed in the communication and information system undergoing assessment. In turn, as per Article 32a(6) of the AISA, in order to minimise the adverse effects of security assessments, the ISA consults the framework conditions for conducting such assessment with a relevant public administration authority, in particular, the commencement date, the schedule, as well as the range and type of security tests performed as part of the assessment. The performance of security assessment may not hinder, or significantly restrict the operations of the public administration authority that is obliged to ensure the continued performance of its tasks. Public affairs must be arranged in an uninterrupted manner, and therefore security assessment cannot be a reason for closing a given office (or its individual organisational units), being a subsidiary entity of a public administration body, if it

becomes impossible to use its communication and information system for an extended period of time. Interference with the operations of a communication and information system of a public administration authority cannot be excessive. It should not result in permanent damage to the data processed in the system, which is required for the tasks performed by such authority.

Under Article 32a(7) of the AISA, the legislators provided the ISA with a possibility to develop or acquire computer hardware or software, and use it to determine the vulnerability of the system being assessed to the risk of the commission of an offence which: 1) results in the endangerment to the lives and health of a large population or property of a significant size, by blocking, or otherwise affecting automatic processing, collection or transmission of IT data (Article 165 § 1(4) of the PC; 2) includes the fixture and/or use of an eavesdropping device, visual device or other type of device or software with a view to obtaining unauthorised access to information (Article 237 § 3 of the PC). This provision penalises the interception of computer data during transmission (Radoniewicz, 2019: 203); 3) includes unauthorised destruction, damage, deletion, change and/or obstructed access to IT data, or significant disruption or prevention of the automatic processing, storage and/or transmission of such data - including activities causing significant damage (Article 268a § 1-2 of the PC; 4) includes the destruction, damage, deletion and/or change of IT data of significant importance to the state defence capabilities, security in communication, the functioning of public administration, other state bodies or local government institutions, or the disruption or prevention of the automatic processing, storage and/or transmission of such data – by destroying or replacing a computer storage medium, or by destroying or damaging a device used for the automated processing, storage and/or transmission of IT data (Article 269 § 2 of the PC); 5) includes a significant disruption of the operation of an IT system, a communication and information system and/or an ICT network, through the transmission, destruction, deletion, damage, obstructed access and/or change of IT data, without being authorised to do so (Article 269a of the PC). The analysed provision (Article 32a(7) of the AISA) constitutes a justification (Opaliński, Rogalski, Szustakiewicz, 2017: 150).

The activities performed as part of security assessment are defined in § 3(1) of the SAR and they include: 1) passive data collection – collecting online information related to the functioning of the system with impact on its security, 2) semi-passive data collection – collecting information in the system to identify data related to the functioning of the system with impact on its security, in line with the rules applicable to system users, excluding actions which require authentication in the system. These activities may be supplemented by collecting information arising from system architecture analysis; 3) active data collection – collecting information in the system to identify data related to the functioning of the system with impact on its security, using a method which goes beyond the authorisations of a system user, including actions which require authentication in the system, in particular, actions consisting in the enumeration of services, ports, detection

of intermediate devices, the detection of IDS/IPS and firewalls; 4) the identification of vulnerabilities in system architecture and web services – undertaking measures aimed at identifying vulnerabilities to threats based on the collected information about system architecture, provided by the system managing entity.

The information obtained by the ISA in the course of security assessment constitute confidential information protected by law and as such may not be used for the performance of other statutory tasks entrusted to the ISA, and it is subject to immediate destruction in the presence of a committee which draws up minutes of the said action. This obligation is imposed under Article 32a(9) of the AISA. The Head of ISA orders that the materials be destroyed immediately upon the completion of security assessment. He/she appoints three committee members taking part in the destruction of materials. The committee is composed only of officers who are members of the ISA organisational unit that performs the security assessment. The materials must be destroyed through: 1) permanent removal of information recorded on computer storage media or their copies on which the information has been saved, in a way which makes it impossible to recover the contents of the recorded data; 2) physical destruction of materials and documents drawn up on their basis, with the use of a shredding device, in a way which makes it impossible to read the contents. The above rules are stipulated in §§ 2 and 3 of the Regulation of the Prime Minister of 18 July 2016 on the methods of destroying materials containing information obtained in the course of security assessment performed by the Internal Security Agency, and on the templates of the required documentation (Polish Journal of Laws of 2016, Item 1055).

If it is found that a terrorist incident has occurred in respect of communication and information systems of public administration authorities that are significant for the continuity of state functioning, The Head of ISA, under Article 32b(1) of the AISA, may request the system managing entity to provide information about the design, functioning, and operating principles of the communication and information systems in their possession, including information on computer passwords, access codes and other data enabling access to the system and its use, with a view to preventing and responding to terrorist incidents affecting such systems, and to preventing and investigating terrorist offences in this sphere, and prosecuting their perpetrators. The information is required for the ISA's performance of its statutory tasks. Pursuant to Article 32b(1) of the AISA, the information is subject to protection as stipulated in the provisions governing the protection of classified information, and may only be disclosed to ISA officers who run investigative operations as part of the given proceedings, and to their superiors who are authorised to supervise the said activities. As per Article 1(1) of the Act of 5 August 2010 on the protection of classified information (consolidated text, Polish Journal of Laws of 2019, item 742, as amended), classified information means those pieces of information whose unauthorised disclosure would or potentially might result in damage suffered by

the Republic of Poland, or would be detrimental to its interests, also in the course of the development of such information, notwithstanding its form and means of expression.

4 An early warning system for threats on the Internet

With a view to preventing, counteracting and combating terrorist incidents which affect communication and information systems of public administration authorities that are significant for the continuity of state functioning and/or ICT networks which are included in the uniform list of facilities, installations, devices, and services which comprise critical infrastructure, as well as the communication and information systems belonging to the owners, owner-like possessors or lessees of critical infrastructure facilities, installations and devices, or of the data processed in the said systems, as well as to prevent and investigate terrorist offences affecting this sphere, and to prosecute the perpetrators of such offences, under Article 32aa (1) of the AISA, the ISA is obliged to implement in the said entities an early warning system for threats on the Internet, as well as to manage and coordinate its operations. The implementation of an early warning system for threats on the Internet is aimed at combating terrorism. Given the above, public administration authorities are obliged to join the early warning system and provide the ISA with required information allowing the implementation of the early warning system in these entities. This obligation is imposed under Article 32aa(4) of the AISA.

As a rule, the early warning system within the infrastructure of a given public administration authority is implemented on the basis of the annual plan. As stipulated in § 2 of the Regulation of the Prime Minister of 2 January 2020 on the conditions and procedure for managing, coordinating and implementing an early warning system for threats on the Internet (Polish Journal of Laws of 2020, item 54), hereinafter "the REWS", the ISA provides a public administration authority where the early warning system is to be implemented in line with the annual implementation plan with information about: 1) the technical aspects of participating in the early warning systems, which are required for its implementation, in particular, start up; 2) the proposed time limit for the implementation of the early warning system.

By way of an understanding, the ISA consults and agrees upon, with a given public administration authority, the technical aspects of participating in the early warning system and the system configuration model. The ISA does not impose its vision of this body's participation in the early warning system, but enters into negotiations with a view to establishing a common position in this respect. Nonetheless, where it is impossible to reach an understanding for reasons attributable to the public administration authority, pursuant to Article 32aa (8) of the AISA, the ISA must notify a supervisory authority or the minister in charge of computerisation.

Participation in the early warning system is subject to the fulfilment of obligations arising from § 5(1) of the REWS, namely: 1) the obligation to immediately remove any malfunctions of network infrastructure powering the early warning system, to maintain its full working order; 2) to monitor and analyse, using own resources, the information generated by the early warning system in order to undertake remedial and safeguarding measures covering the said system; 3) to refrain from providing information to other entities: a) information about the early warning system, b) the whole or part of the software and hardware platform provided by the ISA, c) information about the hardware platform forming part of the early warning system, and about the technical aspects related to the design and operation of the system.

5 Conclusions

Counteracting threats in the cyberspace, including cyberterrorism, will be possible if a high level of security is maintained in communication and information systems of public administration authorities which are significant for the continuity of state functioning and/or ICT networks that are included in the uniform list of facilities, installations, devices, and services which comprise critical infrastructure, as well as the communication and information systems belonging to the owners, owner-like possessors or lessees of critical infrastructure facilities, installations and devices, or of the data processed in the said systems.

In Article 32e of the AISA, the legislators have introduced the recommendation institution, whose aim is to increase the level of security of communication and information systems. The Head of ISA carries out the analysis of incidents that compromise the security of communication and information systems, and issues recommendations to public administration authorities in order to increase the level of security of communication and information systems with a view to ensuring their integrity, confidentiality, accountability and accessibility. The public administration body concerned may submit its reservations to the recommended methods for increasing the level of security of its communication and information systems due to the adverse effects of the recommended measures on the functionality of the system or the occurrence of new vulnerabilities, though no later than within 7 days of the date it receives the recommendations. The Head of ISA expresses his/her position on the reservations, and upholds the recommendations in question, or provides amended recommendations. The body that has received the recommendations must notify the Head of ISA on the method and range of their implementation within a month of their receipt. The failure to implement the recommendations constitutes grounds for the Head of ISA to notify the authority supervising the operations of the public administration authority concerned that the recommendations are not taken into account, or to request that action be taken to implement the recommendations.

References:

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) *Cyberodpowiedzialność* (Toruń: Wydawnictwo Adam Marszałek).

Chałubińska-Jentkiewicz, K., Karpiuk, M. & Kostrubiec, J. (2021) *The Legal Status of Public Entities in the Field of Cybersecurity in Poland* (Maribor: Lex Localis), https://doi.org/10.4335/2021.5.

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.

Hoffman, I. & Cseh, K. (2020) E-administration, cybersecurity and municipalities – the challenges of cybersecurity issues for the municipalities in Hungary, *Cybersecurity and Law*, 2, pp. 199-211.

Karpiuk, M. (2021) Cybersecurity as an element in the planning activities of public administration, *Cybersecurity and Law*, 1, pp. 45-52.

Opaliński, B., Rogalski, M. & Szustakiewicz, P. (2017) *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz* (Warszawa: C.H.Beck).

Radoniewicz, F. (2019) Przestępstwa komputerowe w polskim Kodeksie karnym, *Cybersecurity and Law*, 1, pp. 193-212.