The Role of the State and Public Administration in the Cybersecurity System

TOMASZ ZDZIKOT

Abstract Following the guidelines of satisfying collective needs and acting by the administration in the public interest, it should be pointed out that security is one of the most important individual and collective needs. Ensuring cybersecurity is, therefore, one of the state's tasks carried out with the help of public administration to meet the collective and individual need for security. There is no doubt that in order to perform its tasks effectively in a changing security environment and to meet new challenges, public administration must undergo a series of structural and functional transformations. The state is obliged to ensure appropriate organisational, human and technical resources, which are necessary for the implementation of tasks. The objective awareness of threats and international obligations, and national legal regulations, as well as strategic documents, require far-reaching commitment in this respect.

Keywords: • public administration • cybersecurity • strategy

CORRESPONDENCE ADDRESS: Tomasz Zdzikot, President of the Management Board of Poczta Polska SA, Ul. Rodziny Hiszpańskich 8, 00-940 Warszawa, Poland, e-mail: tomasz@zdzikot.pl.

https://doi.org/10.4335/2022.2.2 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

1 Public objectives and tasks

The doctrine of law distinguishes three basic meanings of the term "administration", among which the first one assumes, as the basic determinant, the organisational structures set up in the state to pursue public task objectives, the second refers to the activities conducted with a view to accomplishing public task objectives, while the third takes into account people employed in organisational structures (Boć, 2010: 12).

The terms "public purpose", "public task" and "public interest" are indeterminate and changeable, depending on the political and social conditions, legal contexts, as well as the system of values accepted as the basis for the functioning of administration in a given time and place. Appearing in lower- and higher-level legal acts, constitutional acts, and substantive and procedural acts, the terms in question play a special role and are most often interpreted as determinants of the permissible scope of interference in the sphere of rights of the an individual and his/her personal interests. The terms "public purpose" and "public interest" have not been defined in a universal way, which results from their nature being relativised subject to changeable external conditions. Hence, the Polish Constitution not only lacks a definition of public purpose, but also does not specify any circumstances under which particular purposes could be deemed public. According to the Polish Constitutional Tribunal, "Whatever serves the commonalty, is generally available or represents the interest of the whole society or regional community, can be deemed public purpose" (Constitutional Tribunal, 2015).

The doctrine emphasises that the meaning of the term "public purpose", as determined on the basis of the above guidelines, may not be subject to extensive interpretation, while its scope may cover only the most common categories of matters connected with satisfying the needs of the population. Deliberations on the essence of public purpose thereby coincide with the category of public tasks. The term "public task" is also deemed indeterminate although tasks are always determined on the basis of binding legal norms. As it has already been mentioned, public tasks are defined by public purposes which public administrations are obliged to meet, whilst the purposes are associated with the public interest. The doctrine points out that the public character of a task means, on the one hand, that it has a normative basis and that, in carrying it out, the state (local government) acts in the public interest – for the common good, construed as certain basic values of a given community. Simultaneously, assigning to a specific task the quality of a public task will imply the recognition that their performance belongs to the duties and not to the powers of public authorities (Strożek-Kucharska, 2016: 122-123). In this approach, public tasks are, first and foremost, constitutional duties of state (local government) authorities, the scope of which cannot be unilaterally limited for political or economic reasons, nor can the state (local government) derogate from their performance, since the raison d'être of the state (local government) is precisely to take specific actions in the collective interest (Blaś, 2003:144).

There is no list or time-invariant set of tasks that, by their very nature, have the permanence of the quality of public tasks. However, some authors perceive a sphere of public tasks which are characteristic for the operation of the state and which can be defined as "model" tasks or public tasks in their pure form. These include in particular ensuring external security and internal order, i.e., those tasks whose performance requires coercion.

The term "public task", as well as the terms "public purpose" and "public interest", are commonly interpreted as limiting the scope of legally permissible activity of a public entity. At the same time, it is assumed that satisfying community needs will always have the nature of a public task, which has been confirmed by the Constitutional Tribunal by indicating that public tasks comprise all tasks of the local government, as they aim at satisfying collective needs (Bandarzewski, 2007: 331-332, Constitutional Tribunal, 1994)

2 Ensuring cybersecurity as a task of the state and the administration

Following the guidelines of satisfying collective needs and acting by the administration in the public interest, it should be pointed out that security is one of the most important individual and collective needs. Ensuring security was, historically speaking, one of the basic factors determining the creation of communities, from neighbourhoods, families and tribes, to the state as the most perfect form of ensuring security for individuals and social groups. Viewing the state through the prism of its functions, construed as the course of action, it is recognized that ensuring internal and external security is of primary importance among them (Czuryk, Dunaj, Karpiuk and Prokop, 2016: 17,19). Security is thus clearly one of the basic values to which constitutional norms refer by distinguishing many of its categories, including security of citizens, security of the state, and internal and external security.

The literature emphasises that the purposes and functions of the state are not identical concepts although they remain closely related. This is a primary purpose in relation to the function, which is instrumental in relation to the intended purpose. Since the state is a purpose-driven institution, the question about the purposes of the state is in fact a question about the essence of the state, about why the state exists and what society wants to achieve through this form of organisation. The purpose will, therefore, be the object of the intended action, the indicated state of affairs pursued by the state, what it wants to achieve and meet, while the function will be the course of action of the state that serves to achieve and meet the intended purpose (Safjan, Bosek, 2016). The relation between purposes and tasks is similar, whereby it is noted that both purposes and tasks are closely related to the category of values realised by public administration. In the case of tasks, it is a time-specific assessment of a present state that is being pursued, an object, a fact or an event, in relation to the lawmaker's system of values, while in relation to the purpose it will be an identical assessment of a projected future state (Cieślak, Bukowska, Federczyk Klimaszewski, Majchrzak, 2012: 14).

From the afore-described point of view, it is more appropriate to consider security as a general purpose of the state being pursued through the performance of a number of tasks. As already mentioned, security is one of the most important values for every human being. In the classic A. H. Maslow's pyramid, which defines the hierarchy of needs, security takes the second place, after physiological needs, and before belonging, esteem and self-actualisation. Considering the foregoing, the doctrine rightly states that the role of the state, and consequently the role of public administration, is to organise social life in such a way so that the need for security could be satisfied both in the subjective dimension (where in the narrow sense it applies to a person, and in the broad sense it applies to the society and the state) and in the objective dimension (involving specific types of security, i.e., for example, energy, financial or transport security) (Czochowski, 2014: 274-275). Cybersecurity must also be considered in this sense. In terms of the object, it covers an increasingly broad spectrum related to the creation of "cyberspace" aggregating hardware, software, networks, systems and human activity in this environment, while in terms of the subject, in connection with the ongoing processes of digitisation, cybersecurity threats may harm both individuals and communities as well as organisations or, finally, states. Hence, it is reasonable to treat cybersecurity (ICT security) as common welfare, leading to the necessity to "create a special legal protection system, under which certain obligations must be assigned to public administration authorities performing regulatory functions and to telecommunication entrepreneurs, while ICT security itself should be subject to either criminal or criminal and administrative legal protection – depending on the gravity of the action affecting it". (Czyżak, 2014: 288).

3 Obligations of NATO Allies

Given the framework of this study and the breadth of the issue at hand, the international implications will be discussed in the outline referring to the most relevant issues of topical nature. From the perspective of the involvement of the state and public administration in cybersecurity efforts, the decisions made in 2016 were crucial in the international arena.

Firstly, cybersecurity issues were among the leading issues at the NATO Summit held in Warsaw on 8-9 July 2016. In the final declaration of the Summit, the heads of the Allies stated that they had committed to "to enhance the cyber defences of our national networks and infrastructures, as a matter of priority" (NATO, 2016a). Simultaneously, NATO expected that "Each Ally will honour its responsibility to improve its resilience and ability to respond quickly and effectively to cyber attacks, including in hybrid contexts". (NATO, 2016a) The theses formulated in the final declaration were developed in the Cyber Defence Pledge, also adopted at the Summit (NATO, 2016b). In this document, in recognition of the new realities of the security threats to NATO, the Heads of State and Government pledged to ensure that the Alliance keeps pace with the rapidly evolving cyber threat landscape and that NATO nations will be capable of defending themselves in cyberspace as in the air, on land and at sea. They also reaffirmed their national

responsibility, in line with Article 3 of the Washington Treaty, to enhance the cyber defences of national infrastructures and networks, and their commitment to the indivisibility of Allied security and collective defence. The Cyber Defence Pledge also lists seven specific commitments which the Allies are required to fulfil:

I. Develop the fullest range of capabilities to defend our national infrastructures and networks. This includes: addressing cyber defence at the highest strategic level within our defence related organisations, further integrating cyber defence into operations and extending coverage to deployable networks;
II. Allocate adequate resources nationally to strengthen our cyber defence capabilities;
III. Reinforce the interaction amongst our respective national cyber defence stakeholders to deepen co-operation and the exchange of best practices;
IV. Improve our understanding of cyber threats, including the sharing of information and assessments;
V. Enhance skills and awareness, among all defence stakeholders at national level, of fundamental cyber hygiene through to the most sophisticated and robust cyber defences;
VI. Foster cyber education, training and exercising of our forces, and enhance our educational institutions, to build trust and knowledge across the Alliance;
VII. Expedite implementation of agreed cyber defence commitments including for those national systems upon which NATO depends (NATO, 2016b)

To ensure that the commitments outlined in the Cyber Defence Pledge would not become an empty declaration, a monitoring system was also envisaged. Thus, it was agreed that progress on the fulfilment of the commitments would be tracked and reviewed on an annual basis. A detailed questionnaire was created for this purpose, on the basis of which the Allied states carry out self-assessment, taking into account the changes in individual countries, including, for example, organisational, structural or legal changes. NATO may also ask additional questions in the area of interest (the so-called Focus Area). On the basis of the data collected this way, enriched with information obtained during bilateral meetings, a report is created containing an assessment of the fulfilment of the commitments included in the Cyber Defence Pledge, which is presented annually during meetings of NATO defence ministers. The report takes into account, among other things, weaknesses and recommendations, and each Allied state receives individual feedback from NATO.

4 Obligations of EU Member States

Additionally in 2016, 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, referred to as the NIS Directive, was adopted. The essence of the regulation was to oblige all European Union Member States to guarantee a minimum level of national capabilities in the area of ICT security. The

provisions of the directive revolve around three pillars: institutions, European cooperation and obligations in the field of network and information security (Wrzosek, 2016). In the first area especially, although not only, the obligations of Member States to act in the sphere of cybersecurity are emphasised. EU Member States have thus been obliged to:

- designate at least one national competent authority on the security of network and information systems (also from among the existing authorities), whose primary task is to monitor the application of the Directive at the national level, by means of a set of minimum powers which the Directive requires competent authorities to have at the national level,
- designate a national single point of contact on the security of network and information systems (also from among the existing authorities), which will exercise a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States, and with the Cooperation Group and the CSIRT network set up under the Directive,
- designate at least one Computer Security Incident Response Team (CSIRTs), comply with the requirements set out in the Annex to the Directive, which will be responsible for risk and incident handling in accordance with a well-defined process, at least for the digital sectors and services described in the Directive,
- develop and adopt a national strategy on the security of network and information systems defining the strategic objectives and concrete policy actions to be implemented.

Importantly, the Directive contains several obligations for Member States to provide the necessary tools and resources, especially to the competent authorities, the single points of contact and CSIRTs to ensure that they carry out, in an effective and efficient manner, the tasks assigned to them, and thereby to fulfil the objectives of this Directive. It should be highlighted that technical, financial and human resources are indicated explicitly.

It is also worth noting at this point that on 16 December 2020 the European Commission presented, *inter alia*, a proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 – being a revised version of the NIS Directive, i.e., the so-called NIS Directive 2 (European Commission, 2020). What draws attention to the catalogue of proposed changes is, *inter alia*, the extension of the subjective scope of the Directive to sectors not previously covered by the NIS Directive. The NIS 2 project takes into account two types of entities: essential entities and important entities. Especially with regard to the latter, the change is noticeable. From among the six sectors in which important entities should operate, only digital providers have been included in the scope of the Directive. The scope of obligations imposed by the NIS 2 Directive on both essential and important entities will also increase significantly. Among the numerous obligations, it indicates, inter alia, the need to ensure supply chain security. Great importance is also attached to certification. The proposal assumes that Member States may require essential and important entities to certify certain products, services and processes under specific European cybersecurity certification schemes provided for in the Cybersecurity Act.

The above changes are closely linked to a significant extension of the tasks of national authorities competent for cybersecurity, which are to exercise supervision over essential and important entities. This, in turn, will mean that national cybersecurity structures will have to be built more dynamically and that EU Member States will have to ensure an adequate level of funding for the tasks imposed on public administration. As experts note, the new tasks will require large resources on the part of public administration, while the sectoral approach to supervision adopted in Poland, combined with the obligation to establish sectoral CSIRTs, will necessitate the allocation of significant funds for this purpose within the state budget (Wrzosek, 2020).

5 Polish solutions in outline

In Poland, the NIS Directive was implemented by way of the Act of 5 July 2018 on the National Cybersecurity System. As indicated in the explanatory memorandum to the proposal for this Act, the comprehensive regulation of the national cybersecurity system results "on the one hand, from the need to ensure a systemic approach to the national cybersecurity system in the face of constantly growing and dynamically changing threats to the operation of the state, economy and society, and, on the other hand, from the need to implement Directive 2016/1148 into the Polish legal order" (Council of Ministers, 2018).

The scope of action of the state and its administration is, therefore, defined in Poland in:

- national legislation of various rank – from the Constitution, through the Act on government administration departments, to the Act on the National Cybersecurity System, which, as mentioned above, implements the provisions of the NIS Directive, together with the implementing acts,
- strategic documents, including in particular the "Cybersecurity Strategy of the Republic of Poland for 2019-2024", which was approved by the Council of Ministers on 22 October 2019 and signed by the Prime Minister on 29 October, effective from 31 October 2019. The strategy superseded the previous "National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022",
- international agreements and commitments, such as the afore-described NATO Cyber Defence Pledge.

The national cybersecurity system that has been shaped and developed in Poland is decentralised. The performance of tasks in this area belongs to many entities, and their effectiveness depends on the cooperation of the units and individuals involved (Zdzikot, 2018: 249).

Pursuant to Article 146 (4), (7), (8) and (11) of the Constitution of the Republic of Poland, the Council of Ministers is responsible for ensuring the internal and external security of the state, as well as public order, and exercises general control in the field of national

defence. The basic divisions within the Council of Ministers was introduced by the Act of 4 September 1997 on government administration departments, which preordains that cyberspace security in the civilian dimension belongs to the department of "computerisation", which is today headed by the President of the Council of Ministers, while historically it was under the competence of the Minister of Digitalisation (whose ministry is currently not a separate department within the government), whilst cyberspace security in the military dimension is part of the department of "national defence", headed by the Minister of National Defence.

Under the Act on the National Cybersecurity System, in the above-described underlying issues resulting from the NIS Directive, the following solutions were introduced into the Polish system:

- with regard to the designation of competent authorities for network and information systems security, the regulatory model adopted in the Act provides for an extension of the competences of sectoral authorities in the field of cybersecurity, instead of establishing a single national cybersecurity authority at the central level. Responsibilities of an administrative, regulatory and control nature have been assigned to ministers competent for the sectors listed in the NIS Directive;
- the operation of the Single Point of Contact is the responsibility of the minister in charge of computerisation;
- in accordance with the requirements set out in the NIS Directive, three Computer Security Incident Response Teams have been established, headed by the Minister of National Defence (CSIRT MON), the Head of the Internal Security Agency (CSIRT GOV) and by the Research and Academic Computer Network - National Research Institute (CSIRT NASK);
- the "Cybersecurity Strategy of the Republic of Poland for 2019-2024" is being implemented, the main objective of which is "to increase the level of resilience to cyber threats, as well as the level of information protection in the public, military and private sectors and to promote knowledge and good practices to enable citizens to better protect their information".

As already mentioned, apart from legal regulations, strategic documents also, or perhaps especially, reflect the way the state perceives its role in the area of cybersecurity, as well as the directions of intervention, which with the help of the administration will be applied to achieve the objectives. The Polish Strategy for 2019-2024 identifies five specific objectives:

1) Developing a national cybersecurity system;
2) Increasing the level of resilience of information systems of the public administration and the private sector, and achieving the capacity to effectively prevent and respond to incidents;
3) Increasing the national capacity in the area of cybersecurity technology;
4) Building public awareness and competences in the area of cybersecurity;
5) Building a strong international position of the Republic of Poland in the area of cybersecurity.

Within the framework of the National Cybersecurity Strategy, the Ministry of Defence has also implemented its own programme since 2019, which fits in with and complements it, and which has identified, within a wide-ranging programme called CYBER.MIL.PL, four core areas of activity:

1) the consolidation and building of cybersecurity structures,
2) education, training and coaching,
3) cooperation and building a strong international position, and
4) increasing the level of security of ministerial and military networks and systems (Complete information including summaries of the individual stages of implementation is available at www.cyber.mil.pl).

6 Summary

Ensuring cybersecurity is, therefore, one of the state's tasks carried out with the help of public administration to meet the collective and individual need for security. There is no doubt that in order to perform its tasks effectively in a changing security environment and to meet new challenges, public administration must undergo a series of structural and functional transformations. The first widely commented and described digital attacks on critical infrastructure date back to the mid-1990's (for example, in 1997, an attacker disabled telephone lines at the Worcester Airport (USA), which were used by the control tower, the airport security services, the airport fire brigade, and the weather service. The runway lighting system was also disabled). Today, the activities of the state and public administration aiming at ensuring cyberspace security are forced not only by the general awareness of threats, but also by international, Union and national legal regulations and strategic documents.

At the same time, ensuring security in cyberspace, in its individual and collective dimension, is a cross-cutting task, the implementation of which rests with a number of authorities and units, especially bearing in mind that the national cybersecurity system constructed by the Polish legislator is not centralised.

In view of the above, the tasks of the state and public administration include, in particular, constructing appropriate mechanisms, processes and procedures for the whole system to ensure, and to continuously improve, the level of cybersecurity against any changing threats. The specificity of this area means that not only command and control powers, but also those from the sphere of dominion, play an important role. The state is obliged to ensure appropriate organisational, human and technical resources, which are necessary for the implementation of tasks. The objective awareness of threats and international obligations, and national legal regulations, as well as strategic documents, require far-reaching commitment in this respect.

References:

Bandarzewski, K. (2007) Prywatyzacja zadań publicznych, In: Zimmermann, J. (ed.) *Koncepcja systemu prawa administracyjnego* (Warszawa: Wolters Kluwer Polska), pp. 331-345.

Błaś, A. (2003) Zadania administracji publicznej. Zadania administracji publicznej w państwie prawa, In: Błaś, A., Boć, J. & Jeżewski, J. (eds.) *Administracja publiczna* (Wrocław: Kolonia Limited), pp. 139-144.

Boć, J. (ed.) (2010) *Prawo administracyjne* (Wrocław: Kolonia Limited).

Chochowski, K. (2014) Bezpieczeństwo publiczne jako dobro publiczne, In: Woźniak, M. & Pierzchała, E. (eds.) *Dobra publiczne w administracji* (Toruń: Adam Marszałek), pp. 265-279.

Cieślak, Z. (ed.), Bukowska, J., Federczyk, W., Klimaszewski, M. & Majchrzak, B. (2012) *Nauka administracji* (Warszawa: LexisNexis).

Czuryk, M., Dunaj, K., Karpiuk, M. & Prokop, K. (2016) *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne* (Olsztyn: WPiA UWM).

Czyżak, M. (2014) Bezpieczeństwo teleinformatyczne jako dobro publiczne i wybrane aspekty jego prawnej ochrony, In: Woźniak, M. & Pierzchała, E. (eds.) *Dobra publiczne w administracji* (Toruń: Adam Marszałek), pp. 286-298.

NATO (2016a) *Deklaracja końcowa szczytu NATO w Warszawie Wydana przez Szefów Państw i Rządów uczestniczących w posiedzeniu Rady Północnoatlantyckiej w Warszawie w dniach 8 i 9 lipca 2016 r.*, available at: https://www.bbn.gov.pl/ftp/dok/03/37-40_KBN_Deklaracja_szczytu.pdf, https://www.nato.int/cps/en/natohq/official_texts_133169.htm (August 30, 2022).

Safjan, M. & Bosek, L. (eds.) (2016) *Konstytucja RP. Tom I. Komentarz do art. 1–86* (Warszawa: C.H. Beck).

Strożek-Kucharska, M. (2016) Definiowanie zadań publicznych – wprowadzenie do dyskusji, In: Bieś-Srokosz, P. (ed.) *Zadania publiczne. Podmioty-uwarunkowania prawne-potrzeby społeczne* (Częstochowa: Wydawnictwo im. S. Podobińskiego, Akademii im. Jana Długosza w Częstochowie).

Wrzosek, M. (2016) *Dyrektywa NIS, czyli pierwsze europejskie prawo w zakresie cyberbezpieczeństwa* (NASK), available at: https://cyberpolicy.nask.pl/dyrektywa-nis-czyli-pierwsze-europejskie-prawo-w-zakresie-cyberbezpieczenstwa/ (August 30, 2022).

Wrzosek, M. (2020) *Dyrektywa NIS 2 – jakie zmiany w zakresie cyberbezpieczeństwa proponuje Komisja Europejska?* (NASK), avalable at: https://cyberpolicy.nask.pl/dyrektywa-nis-2-jakie-zmiany-w-zakresie-cyberbezpieczenstwa-proponuje-komisja-europejska/ (August 30, 2022).

Zdzikot, T. (2018) Państwo i administracja publiczna na straży cyberbezpieczeństwa, In: Federczyk, W. (ed.) *Stulecie polskiej administracji. Doświadczenia i perspektywy* (Warszawa: Krajowa Szkoła Administracji Publicznej im. Prezydenta Rzeczypospolitej Polskiej Lecha Kaczyńskiego).