Cybersecurity as a Public Task in Administration

KATARZYNA CHAŁUBIŃSKA-JENTKIEWICZ

Abstract The protection of citizens and the state against threats is the constitutional obligation of all authorities, including state administration and local government authorities. The tasks which result from this obligation involve the prevention, identification and elimination of all forms of threats to the population of a given territory. Contemporary states, whose administration relies on modern technology, have become vulnerable to interferences which disrupt information processes, as well as the databases, devices and ICT networks whose functioning depends on these processes. Cyberspace security requires that appropriate methods are in place to ensure the secure processing, storage and transmission of information resources available in communication and information systems. Hence, ensuring network security represents a major task for the public administration of the state.

Keywords: • cybersecurity • cyberspace • public administration • public tasks

CORRESPONDENCE ADDRESS: Katarzyna Chałubińska-Jentkiewicz, Ph.D., Dr. Habil., Associate Professor, War Studies University, Law Institute, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warsaw, Poland, email: k.jentkiewicz@akademia.mil.pl.

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

1 Cybersecurity in public administration – general remarks

Numerous processes have shaped the contemporary public administration environment in Poland. The political transformation which took place in Central and Eastern Europe after 1989 had a global range. It was an attempt at simultaneously restoring political freedom, private ownership and a market economy environment, as well as the mechanisms and values of the civic state. This period was marked by the gradual reconstruction of the Republic of Poland's statehood based on the principles of a democratic state of law, a social market economy based on the ownership right, among other things, and of respect for individual freedoms. The state system and political considerations have contributed to the transformation of the centrally planned economy into a free market economy. After new quality management systems had been implemented, it became a requirement for administration structures to provide high-quality public services. Relying on new technologies, the critical infrastructure of the state became vulnerable to various types of incidents and associated threats. The contemporary state, whose administration uses new technological solutions for its day-to-day work, has become prone to device, IT network, system and database disruptions, affecting information processes (Hoffman & Cseh, 2020: 200). Ensuring the security of information resources and systems used to perform public tasks has become a serious issue. In order for public sector entities to function efficiently, it is a prerequisite that public tasks related to ensuring cybernetic security be implemented at each stage of public institutions' operations (Szczepaniuk, 2016: 7).

2 The concept of public administration

It is impossible to discuss cybersecurity issues without first describing the environment in which public tasks related to cyberspace protection are implemented by public administration authorities. Therefore, before the term "cybersecurity" can be defined, it is necessary to explain the concept of public administration.

One of the core objectives of public administration is to provide public services. The early formative years of administrative structures were also marked by the emergence of many theories and doctrines of administration. Various political, social, and economic conditions have shaped the contemporary public administration models. The functioning of administration should also be considered in the context of the changes and conditions in its environment, which underwent considerable transformations over the centuries. Contemporarily, there has been a general trend towards a shift from the administration to the management of public affairs, as reflected by the introduction of the concept of "good governance" in the public sector (Szczepaniuk, 2016: 8).

The term "administration" derives from the Latin word "ministrare", which means to lead, serve, manage[1] (and the prefix "ad" emphasises the service-related aspect) (Ochendowski, 2002: 18, Izdebski, Kulesza, 2004: 23, Hausner, 2005). One of the first

[1] Latin *administratio* – administrating, managing; *administrare* – to be of assistance.

definitions was put forward by W. Jellinek at a time when the "state of law" was emerging, and referred to the tripartite separation of powers in the state. It proclaimed that administration is an activity of the state which is neither legislation nor justice" (Szczepaniuk, 2016: 11).

Public administration has been extensively defined by legal commentators, but all these definitions relate to the state (or local government), society, and the citizen. J. Starościak (Starościak, 1975) describes it as an organisational function with features such as the initiating nature of activities, solving specific situations, and carrying out organisational work, not only by creating binding norms within the legal order, specific legally defined forms of administrative activity of the state (Lisiak-Felicka, Szmit, 2016: 55). According to H. Izdebski and M. Kulesza "Public administration is understood as a set of activities, operations and undertakings, both organisational and executive (the functional element), carried out in the public interest (the object element) by various entities, bodies, and institutions (the subject element) on the basis of Acts, and in the forms specified by law (functional element)" (Izdebski, Kulesza, 2004: 93). Most generally, citing E. Ochendowski (Ochendowski, 2002: 19), this term is understood to mean any organised activity aimed at achieving specific objectives. And according to J. Boć public administration is the fulfilment of the collective and individual needs of citizens, resulting from the coexistence of individuals in communities, by the state and its dependent authorities, as well as by local authorities (Boć, 2004: 16).

Public administration is defined as a set of activities, operations, and organisational and executive undertakings carried out in the public interest by various entities, bodies and institutions, on the basis of Acts and in the forms established by law. It serves the general public and covers the scope of matters of a public nature (Monarcha-Matlak, 2008: 19). In defining public administration, we therefore refer to functions and actions which link the administration to its active and state-dependent activities. State and local government authorities establish organisational structures to meet the needs of citizens. The computerisation process, which is being introduced with a view to facilitating the effective performance of public services and tasks, is a means by which modern administration intends to meet such needs.

Public administration is a complex phenomenon which belongs to the sphere of state-apparatus organisation and functioning. It is established to have various entities operating under law perform public tasks. There are many approaches to dividing public administration. The one proposed by H. Izdebski and M. Kulesza divides administration into centralised state administration, centralised public administration and non-administration entities assigned with public tasks.

According to this classification, public tasks are performed 1) for state administration – by a hierarchical and centralised government administration; 2) on a decentralised basis – by independent institutions and other public administration entities; 3) as tasks assigned

to various institutions, organisations and other entities, especially those operating outside the public sector (Lisiak-Felicka, Szmit, 2016: 56).

Public administration can be compared to an organisation. An organisation denotes an institution, functional group or organisational process (Szreniawski, 2004: 30). The establishment of an organisation's structure depends on the resources, specific goals and conditions for implementation in the system. An organisation is a multi-stage and complex process encompassing functional objectives, the coordination and verification of activities, and the division and specialisation of labour (Władek, 2013: 36-46.) Public administration as an organisation is a social system created by people who serve specific functions in the organisational structures and contribute to the defined objectives through specific modes of action and physical measures. Public administration performs specific activities, operations and undertakings in accordance with applicable law and in forms prescribed by legal norms (Szczepaniuk, 2016: 12-15). Each public administration entity has specific operational objectives implemented in the public interest and to meet social needs using available resources. In order to complete these tasks public administration has a specific structure, which constitutes a set of interrelations between its individual components. The administration system follows specific decision-making rules and organisational techniques comprising specific rules, procedures and practices. These characteristics define public administration as a system of operations (Szczepaniuk, 2016: 12-15). The efficient and effective functioning of public administration depends to a significant extent on its organisational structure, which consists of various units vested with the powers specified in the Acts, and forming a specific organisational system to perform public tasks (Lang, 1997: 15).

According to E. Szczepaniuk public administration in Poland can be outlined along five core systems: 1) the structure of the public administration system – a mechanism of compatible and collaborative public administration entities functioning across the state; 2) the structure of the government administration system – a mechanism of compatible and collaborative government administration entities; 3) the structure of local government administration – associated with the territorial division of the country and comprising a mechanism of compatible and collaborative local government units; 4) the structure of administration as divided into departments; 5) the structure of an individual public administration entity (Szczepaniuk: 2016: 15).

The transformations associated with computerisation and the popularity of information and communication technologies[2] ("ICT") have resulted in, among other things, the convergence of economic, social, and political phenomena. On the one hand, the duty of public administration in the information age is to synchronise the activities of entities

[2] Information and communication technologies (ICT) – all activities relating to the manufacture and use of telecommunications- and information-technology equipment and associated services, and the collection, processing, and provision, of information in electronic form using digital technologies and any electronic communication tools http://lawp.eu/pdf/ict_definicja.pdf.

belonging to various sectors, to manage complex social networks, and to adapt the functioning of public administration to the use of new technologies.

Like other EU states, Poland has embraced the notion that the functions of new ICTs should drive the social and economic progress of the country. And a significant role in this progress is attributed to the operational transformations of public administration so that it is based on citizen-friendly and transparent administrative structures relying on ICT. When describing public administration in the information age, it should be noted that it is one of the most important users of modern ICT tools and techniques, since the functioning of the administration involves, or is based on, the processing of information; information is, therefore, an essential resource for administration (Szczepaniuk, 2016: 26).

3 Public tasks in administration

Administration constitutes a separate organisational structure comprising various units and entities vested with statutorily defined powers and forming a certain organisational system whose purpose is to perform public tasks (Lang, 1997: 15).

In a democratic state of law public administration tasks have the status of legal obligations. They are set out by the Constitution of the Republic of Poland of 2 April 1997 (Polish Journal of Laws, No. 78, item 483, as amended) ("the Constitution of the Republic of Poland)" and legal acts passed by competent legislative bodies. In accordance with Article 31 (3)[3] of the Constitution of the Republic of Poland administration authorities may restrict the constitutional rights and freedoms of citizens for the purposes of performing their public tasks. In a state of law, administration can influence the shape of legal acts which contain the legal norms characterising its tasks; however, it may not decide what its tasks are. It may have some freedom and influence on the shape and scope of the tasks to be carried out, but the sources and limits of that freedom always stem from the legislation adopted by the responsible legislative bodies. The functions of administration may also be defined clearly and directly in the Constitution of the Republic of Poland, or emanate from the constitutional norms describing the objectives and functions of the state and civil rights, formulated as a result of the indirect interpretation of the law (Jaxa-Dębicka, 2008: 12).

The state performs its tasks through public authorities. Central and local government authorities, and other state authorities are responsible for public tasks. This is a statutory procedure, followed in the public interest. Polish legislation does not offer any legal

[3] Restrictions in the exercise of constitutional freedoms and rights may be imposed only statutorily and only when necessary for a democratic state to ensure its security or public order, or for the protection of the environment, health and public morality, or the freedoms and rights of other individuals. These restrictions may not, however, undermine the essence of freedoms and rights.

definition of public tasks. However, many definitions can be found in academic papers (Chałubińska-Jentkiewicz, 2014: 20).

Public administration is based on the implementation of public tasks by public entities. On the basis of the definition of public administration presented by J. Boć, "public tasks" can be understood as tasks assumed by the state, consisting of meeting collective and individual human needs resulting from the coexistence of people in communities. The development of communities and the changing reality is enforcing changes to the field of the tasks taken over by the state. These tasks are implemented on the basis of the provisions of the law (Boć, 2014: 17).

According to A. Błaś the performance of administrative tasks is the duty of the public administration authority to which they have been entrusted by law to take up an active role in the implementation of these tasks (Boś, 2014: 44). The literature on the subject stresses that administrative tasks should be supported by the very broadly defined rule of good governance. It is also worth mentioning that public administration can be understood as a set of activities, operations, and organisational and executive undertakings, carried out in the public interest by various entities, authorities, and institutions, on the basis of Acts, and in the forms established by law (Izdebski, Kulesza, 2004: 79).

According to S. Biernat public tasks may be performed by public entities without any powers of authority, or even by non-public entities. The main criterion for defining a task as a public task is the fact that a state or local authority is legally responsible for its implementation. The mere performance of tasks within the organisational structures of the state or local government is not a criterion which qualifies it as public tasks. The responsibility of the authorities is maintained when other entities are authorised to perform public tasks, but the forms of activity and their scope change" (Biernat, 1994: 29-30).

P. Schmidt defines public tasks as a set of activities, operations, and organisational and executive undertakings carried out in the public interest by various entities, bodies and institutions, on the basis of Acts and in forms established by law (2012). And T. Kocowski describes public tasks as a legal obligation for an entity clearly indicated in legal norms to achieve or maintain a certain state which is important and desirable in terms of the public interest (Kocowski: 2012). These two definitions, though different in content, have many compatible properties. Public tasks is a collective term for tasks carried out by the state, which performs them through public administration. Pursuant to applicable law, public tasks are implemented through planned and rational action aimed at reaching specific objectives (Mikicka: 2012).

In J. Zimmermann's view, the main indicator for considering a task public is where the state or local and regional authorities are responsible under law for carrying it out (Zimmermann, 2016). According to M. Stohl the concept of a "public task" is associated

with public (public-utility) objectives to be achieved by administration. In turn these objectives are identified with the public interest (Stahl, 2007). According to E. Knosala there are currently no clear criteria for distinguishing between the public and the private domain. This means that the outlines of public tasks are no longer as clearly defined as in the past (Knosala, 2010). A typical feature of public tasks is that their performance is an obligation of public authorities, not an entitlement. This concept is determined by individual legal norms, which are indeterminate due to the fact that it is the state that decides independently and ultimately whether a given function is a public task or not. It is not necessary for public tasks to be implemented within the structure of public administration (e.g. if the performance of a public task has been privatised). Public tasks are the tasks which serve to meet collective needs and the needs of a particular community (Chałubińska-Jentkiewicz, 2014: 20).

The law provides a legal basis for public administration, and sets out a framework for the performance of public tasks. Respect for the law is based on the constitutional principle of legalism (the rule of law) expressed in Article 7 of the Constitution of the Republic of Poland. "Public tasks" is a legal term used in the Constitution of the Republic of Poland – specifically in Articles 15, 16, 163 and 164 – in the context of the local government's participation in exercising public power, as referred to in Articles 7 and 10. The public tasks mentioned in the Constitution of the Republic of Poland include tasks meant to help "meet the needs of the local government community" and tasks guaranteed by the Constitution of the Republic of Poland, or to help the statutory bodies of other public authorities, including those which may be statutorily assigned to local government authorities where reasonable due to "justified needs of the state" (Martysz, Szpor, Wojsyk, 2015: LEX).

The public tasks mentioned in the Constitution of the Republic of Poland include: 1) guaranteeing the security and inviolability of the territory of the Republic of Poland, human and civil rights and freedoms, the security of citizens, environmental protection – Article 126 (2) of the Constitution of the Republic of Poland; 2) ensuring equal access to publicly funded healthcare services and special healthcare for children, pregnant women, people with disabilities and the elderly – Article 68 (2) of the Constitution of the Republic of Poland; 3) providing support to Poles living abroad and Polish citizens temporarily staying abroad – Article 6 (2) of the Constitution of the Republic of Poland; 4) implementing a full-employment policy – Article 65 (5) of the Constitution of the Republic of Poland; 5) guaranteeing universal and equal access to education for citizens – Article 70 (4) of the Constitution of the Republic of Poland; 6) assisting people with disabilities to ensure their livelihood, adaptation to work and social communication, as well as developing special programmes to take care for veterans of the struggle for independence – Articles 19 and 69 of the Constitution of the Republic of Poland; 7) pursuing policies conducive to satisfying the housing needs of citizens and combating homelessness – Article 75 (1) of the Constitution of the Republic of Poland; 8) providing assistance to families in difficult material and social circumstances – particularly those with many children or a single parent, and protecting children's rights, including care and

assistance from public authorities to children without parental care – Article 71 (1) of the Constitution of the Republic of Poland.

The tasks of public authorities are defined in individual Acts. They involve, for instance, the protection of cultural goods, ensuring the maintenance of cleanliness and order, the organisation of various modes of transport, spatial planning, water supply and wastewater disposal (Martysz, Szpor, Wojsyk, 2015: LEX). According to J. Boć it is clear that regardless of the subject of public tasks, public authorities (including public administration authorities) are obliged to actively plan, organise, perform, and monitor the performance of the tasks assigned to them by law as public tasks. In a constitutional state of law the non-performance or improper performance of administrative tasks leads to political and legal liability (Boś, 2004: 142).

Government administration authorities and local government entities, and other state authorities, are responsible for public tasks, i.e. legally defined conduct postulated for the sake of common good. According to legal commentators public tasks may be performed by public entities without any powers of authority, or even by non-public entities. The main criterion for considering a given task as public is that the state or local authority is legally responsible for its implementation (Martysz, Szpor, Wojsyk, 2015: Lex 10190).

The Constitutional Tribunal (CT), in its Resolution of 27 October 1994, case file No. W 10/93, OTK 1994, No. 2, item 46, ruled that all tasks of local government which serve to satisfy the collective needs of local communities, as well as national needs, were public tasks. According to the CT both assigned tasks and local government's own tasks are public tasks as defined by applicable law. A comparably broad interpretation of "public tasks" has been adopted in case law (K. Chałubińska-Jentkiewicz, 2014: 21).

The Decision of the Supreme Court (SC) of 26 June 1992, III ARN 32/92, states that local governments perform all public administration tasks, whether their own or assigned. The definition of the commune's own tasks as public tasks is not inconsistent with the undoubted fact that the commune, as an entity responsible for the municipal assets, manages these assets in a manner appropriate for the performance of its own tasks. (Kłaczyński, Szuster: 2003). It should be mentioned here that the set of systems which constitute critical infrastructure is also part of the municipal assets. Special tasks in the field of cybersecurity are entrusted to local government entities under the Act of 26 April 2007 on Crisis Management (consolidated text, Polish Journal of Laws of 2017, item 209, as amended). In accordance with Article 3 (2) of the Act on Crisis Management, critical infrastructure should be understood as systems and functionally integrated facilities, including installations, devices, building structures, and services crucial for the security of the state and its citizens, and serving to guarantee the efficient functioning of public administration authorities, as well as of institutions and enterprises (K. Chałubińska-Jentkiewicz, 2014: 21).

Public tasks are the tasks which serve to meet collective needs and the needs of a particular community. Public tasks are generally attributed to the state, but political factors decide which tasks will be performed by its authorities on an exclusive basis, which can (and must) be entrusted to other public authorities, and which can be performed by non-public entities (Dobkowski, 2004: 106).

The primary task of the policing function of the state, often referred to in the literature as "order maintenance and regulatory administration", is to safeguard public order and the common interest. Given the profound significance of these objectives, it can be noted that this function also outlines the scope of responsibilities of public authorities towards citizens. This function includes the use of instruments of authority as an attribute of state authority (administrative permits, orders and police-issued prohibitions) and the maintenance of various services and guards whose role is to protect public order and security (border guard, the military, the police) (Jaxa-Dębicka, 2008: LEX).

Therefore public tasks for the security of cyberspace have high priority in the safe and efficient functioning of the state. The responsibility for ensuring cybersecurity rests with all network users, but public administration authorities have a particularly important role to play, as their priorities include ensuring public security and order. The Council of Ministers, in leading Government administration, performs its constitutional responsibilities by carrying out tasks for the protection of cyberspace. It also has the primary responsibility for ensuring a high level of security for cyberspace and the citizens functioning within it (K. Chałubińska-Jentkiewicz, 2014: 26).

In the existing regulatory environment the Minister of Digital Affairs is responsible for ensuring the observance of the minimum requirements for ICT security in public administration. The relevant provisions can be found in the Act of 17 February 2005 on the Computerisation of the Operations of Entities Performing Public Tasks (consolidated text, Polish Journal of Laws of 2017, item 570, as amended) and the Regulation of the Council of Ministers of 12 April 2012 on the National Interoperability Framework (KRI), the minimum requirements for public records and the exchange of information in electronic form, and the minimum requirements for communication and information systems (consolidated text, Polish Journal of Laws of 2016, item 113). The Minister of Digital Affairs has also approved the Guidelines for Monitoring the Functioning of Communication and Information Systems Used to Implement Public Tasks. The aim of these Guidelines is to support the monitoring of the functioning of communication and information systems used to implement public tasks, including the fulfilment of the above-mentioned information security requirements. In accordance with the Act of 5 September 2016 on Trust and Electronic Identification Services (Polish Journal of Laws of 2016, item 1579) the Minister of Digital Affairs is also obliged to ensure the functioning of the national trust infrastructure and supervise trust service providers.

The Ministry of Digital Affairs is now at an advanced stage of work on introducing a new law to set out the organisation and operational procedures of the national cybersecurity

system. The law being drafted will implement 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 2016 L194. The legislation will also introduce the National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022.

The national cybersecurity system law is aimed at ensuring cyberspace protection at a national level. Also, it is meant to guarantee, among other things, the uninterrupted provision of services that are essential for the state and the economy, as well as digital services, by achieving a high security level for the information systems used to provide these services.

This new regulation will lead to an increased resilience of information technology-based essential services against attacks from cyberspace. Consequently, it will help to ensure the continuity of these services such that both citizens and businesses have permanent and uninterrupted access to them.

The expansion of modern communication and information technologies has meant that the administration is responsible for the quality and maintenance of the associated infrastructure, as it has been traditionally responsible for the quality and maintenance of transport routes and road networks. It is clear that the creation of the technical infrastructure and the system of access to it by specific users requires substantial financial resources, which can only be provided by private entities interested in benefiting financially from this business. In this respect the function of public administration is to ensure the security of information systems and IT networks, and to select entities which ensure the continuity and high quality of services, while guaranteeing access conditions for the widest-possible range of recipients (Jaxa-Dębicka, 2008: LEX).

As already mentioned, one of the primary public tasks is to ensure a safe and efficient state, including the security of cyberspace. Cybersecurity is all the more important because the dangers in cyberspace can adversely affect national security, which in turn is the foundation of public tasks (K. Chałubińska-Jentkiewicz, 2014: 22).

"National security is also the most important value, national need, and priority of the activities of the state, individuals, and social groups, and at the same time a process comprising a variety of measures to ensure sustainable, unhindered, national (state) existence and development, including the defence of the state as a political institution and the protection of individuals and society as a whole, as well as their assets and the natural environment, from threats which significantly restrict its functioning or pose a threat to fundamental rights" (Kitler, 2011: 22-31). The key national needs include needs of a systemic nature (e.g. strengthening the social and economic system and legal order), social needs (ensuring health protection, social security, and counteracting all forms of discrimination), economic needs (e.g. national development, economic growth), ecological needs (environmental protection), and cultural needs (nurturing national

heritage, respect for differences in outlooks on life, and ethnicity) (Kitler, 2011: 37). Each of these national needs can be adversely affected by cyber threats, which is why the security of cyberspace is so important for the proper functioning of the state (Bączek, 2011: 244).

To recapitulate, state administration, as a complex structure, performs public tasks in the field of cybersecurity through a set of activities, actions, and organisational undertakings. The administration's primary tasks include efforts to guarantee public safety and order. It ensures the security of information systems and IT networks, and selects the entities which ensure continuity and a high quality of services, while guaranteeing access conditions for the widest-possible range of recipients. Furthermore, it secures the functioning of the national trust service infrastructure and supervises trust service providers. Public administration carries out activities to serve the public interest through cooperation between public authorities and services. And these authorities are responsible for ensuring a high level of security for cyberspace and its users.

4 Definition of cyberspace

The dynamic civilisational changes which have been observed in the last few years have arisen from a rapid growth in information and supporting ICT technologies. The information revolution, the emergence of the Internet, the development of the information society, the globalisation of almost every sphere of human activity, and the associated rapid progress in ICT have undoubtedly been the primary drivers of the contemporary information environment. Access to new technologies, and the fact that they are so commonly used by the public, have created a need for distinguishing another dimension of physical reality – namely, cyberspace. The convergence of information and communications technologies and the media, which has been intensifying for at least a quarter of a century, and, in consequence, the convergence of the info-, socio- and techno-spheres, have contributed to the emergence of the "cyberspace" phenomenon – a global, timeless space, not defined by geographical and political borders.

The development of the Internet, the worldwide computer network, at the turn of the 21st century, was one of the most significant technological breakthroughs in the history of humanity.

At first it was used exclusively in scientific research; as time went by, and as the tools making it easier to use the Internet were developed, it became a key and fundamental element in the functioning of individuals in all spheres of life (Wojciechowska-Filipek, Ciekanowski, 2016:91). The beginnings of the computer network date back to the Cold War period of the 1960s. In that period a communications system was created in the United States which in 1969 gave rise to the ARPANET (Advanced Research Projects Agency Network), considered to be the prototype of the Internet. Initially, the network connected four computers in the USA. It was used to check connectivity in situations where there was a malfunction of one of its links. Further research and government

centres joined the project over time. A spectacular boom of the Internet and the birth of the Telnet system took place. The system allowed connection with other computers and made it possible to use them remotely the same as local desktops. Eventually, the first e-mail was sent, and intercontinental connection was achieved for the first time. This is how the Internet came about (Pala, 2015). The Internet in Poland dates back to 1991, when connection with the international network was established for the first time through the TCP/IP2 protocol (Werner, 2014: 30).

The combination of information and telecommunications technologies ushered in a new era of global communication. By the end of the 1990s the growth of the Internet had made many spheres of life which were based on computer technology dependent on the Internet. It became a tool whereby people could expand their knowledge, a source of information, and an integration point (Wojciechowska-Filipek, Ciekanowski, 2016: 14). The Internet underwent rapid commercialisation and development. New services sprang into existence – websites, social networks, electronic mail, forums, blogs, search engines, instant messaging, multimedia streaming, to name a few. The expansion of the physical infrastructure of the global network has resulted in a steady growth in the number of Internet users. As the information society continues to develop rapidly and commensurately with the expansion of the reach of the Internet, other areas of human activity extend into cyberspace. Instant access to the Internet from almost every place on Earth, and its worldwide reach, combined with low usage costs, have made more and more entities (governments, institutions and businesses) and individuals move large parts of their daily activities to the virtual network (Grzelak, Liedel, 2012).

The word "virtual" derives from the Latin "virtus" and denotes "one which can exist, theoretically possible" (Grudzewski, Hejduk, 2007: 158). Virtual means implicit, unreal, reminiscent, or having a semblance, of a physical being without being one in reality (Najda-Janoszka, 2010: 37).

According to the Polish Language Dictionary "virtual " is defined as: 1) created in the human mind but probably existing, or having the potential to exist, in reality; 2) created on a computer or TV screen but realistic enough to seem existent in reality.

The term "virtual" is associated with interactive multimedia technologies, which are the consequence of common access to personal computers, the development of the Internet, computer graphics, computer science and technology (Kisielnicki, 2008: 351).

Virtualisation is the transfer of entities from the real (physical) world to an imaginary form of the world perceived and interpreted by humans based on specific, invented assumptions (Trajer, Paszek, Iwan, 2012: 38). Virtualisation is a technology which uses a logical environment to overcome the physical limitations of equipment (Lim, Yoo, Park, Byun, Lee, 2012: 151).

The growing use of communication and information systems by societies around the world, and their importance for critical infrastructure, have made it necessary to formulate the legal definition of cyberspace. It was necessary to explore this unique environment which led to the reinvention of administrative procedures and defined a new dimension of security. The nature and security of cyberspace have become the subject of extensive scientific research.

Cyberspace has become an environment in which contemporary society, especially its young generation, lives and functions. Although still considered a "novelty", the term was first used in the 1980s by W. Gibson, who described it as follows: "A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts [...] A graphic representation of data abstracted from the banks of every computer in the human system [...] Lines of light ranged in the non-space of the mind, clusters and constellations of data" (Gibson, 2009: 59). Indeed, Gibson pointed to some of the distinctive features of the environment: unlimited time and space, virtuality, complexity, and the collation of all resources in one huge database (Szczepaniuk, 2016: 69). Visualisation, or, in Gibson's words, "a graphic representation", has become the defining feature of the subgenre of science-fiction called cyberpunk[4].

At the beginning of the last decade of the 20th century, during the Gulf War (1991), which was reported as "the first information war" (Campen, 1996:11), a thesis emerged that cyberspace had become the fifth environment (besides land, sea, air, and the cosmos) in which combat and warfare were being conducted (Warden's model) (Warden, 1995).

P. Sienkiewicz set out to interpret the essence of the construct called cyberspace. He distinguished the following basic perspectives from which the topic can be approached: 1) cyberspace is essentially a huge social network – a net of nets, the participants in which, either individuals or groups (societies), utilise global resources provided by the Internet (generally speaking, the web); 2) cyberspace is identified with the virtual reality generated by the computer, the network, and the Internet; 3) cyberspace is simply the Internet, its resources, services, and users; 4) cyberspace is merely an evolving, dynamic, complex, system (a system of systems), and it should be seen as such, no matter whether we foreground its technical, informational, or social aspects (Sienkiewicz, 2015).

"In physical terms, cyberspace may be characterised by Maxwell's four equations, which are 1) Gauss's law for electric fields; 2) Faraday's law of induction; 3) Gauss's law for magnetism; 4) Ampère's law (further developed by Maxwell) (Słota-Bohosiewicz, 2015: 155-166).

[4]Cyberpunk is a subgenre of science-fiction literature and cinematography which foregrounds the relationship between man and the advanced technology which surrounds him. The defining feature of the genre is its depiction of a vision of a future in which the environments of people, appliances, and computers start to permeate one another.

The capability of analysing, generating, receiving, and measuring fluctuating electric and magnetic fields was knowingly applied, for the first time, in a device called the telegraph (Słota-Bohosiewicz, 2015: 155-166).

D.E. Denning defines cyberspace (its technical aspect) as the space of information created by all computer networks put together (Denning, 2002: 24). A similar definition is formulated by G. T. Rattray, according to whom it is a physical domain which is the result of the creation of information systems and networks which enable mutual interactions through electronic communication (Rattray, 2004: 30). P. Sienkiewicz defines cyberspace in the technical dimension as the global network made of a time-variable number of constituent networks (TCP/IP), with unlimited and open resources and available services (Sienkiewicz, 2012: 324). In the above definitions cyberspace is related to computer systems operating within computer networks.

One of the definitions of cyberspace cited in literature is the one provided by the United States Department of Defence. According to this definition cyberspace is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, and embedded processors and controllers". The above definition refers merely to the technological dimension of cyberspace. It does not make any references to the social sphere – humans, the users of cyberspace. In addition, the definition underscores the hardware aspect of infrastructure with the leading role of the Internet, whereas the software aspect is overlooked (Szczepaniuk, 2016: 71).

In Europe there is a range of definitions adopted in official documents released by various countries, and by the European Union. The European Commission defines it as the virtual space in which electronic data circulate, and are processed by PCs from all over the world (Wasilewski, 2013: 229). The basic element of this definition relates to virtual space as a data system which is accessed through communication and information systems. The interpretation by the European Commission also disregards the user sphere. Another, more exhaustive definition, of cyberspace is proffered by the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, which says that cyberspace is a time-dependent set of interconnected information systems and people/users who interact with those systems[5].

The need to regulate the matters related to cyberspace security has been reflected in a large number of strategic documents and legislation. NATO's new strategic concept[6] and

[5] R. Otis, P. Lorents, Cyberspace: Definition and Implications, Cooperative Cyber Defence Centre of Excellence, Tallinn. http://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-impications.pdf.
[6] A Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation, Lisbon 2010.
https://www.bbn.gov.pl/download/1/15758/KoncepcjastrategicznaNATO.pdf.

updated cyber-defence policy identify cyber threats, in special cases, as potential reasons for exercising collective defence under Article 5 (Szczepaniuk, 2016: 72).

In accordance with the Polish regulations cyberspace is defined as virtual space in which information is processed and exchanged by information systems, as set out in Article 3(3) of the Act of 17 February 2005 on the Computerisation of the Operations of the Entities Performing Public Tasks (consolidated text, Polish Journal of Laws of 2017, item 570, as amended) ("the Computerisation Act") and the interrelations between the entities and the relationships with users. The Act of 29 August 2002 on 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). Cyberspace is therefore a generalisation of the concepts of "systems" and "ICT networks", which can be visualised with the ISO-OSI layer model[7].

In that respect this definition converges with the one proposed by CCDCoE[8], since it includes both the human and the technical components of cyberspace. One of the essential aims of its amendments was to introduce the category of cyberspace as one of the constituents of national security. The introduction of the definition became especially important to the institutions and authorities which were in charge of broadly understood security, allowing one to create an "instrumentarium" of powers, necessary for those entities to perform tasks in accordance with the constitutional principle of legalism. The solutions adopted complied with NATO's Strategic Concept of 2010, which was in effect at that time, and at the same time they complemented the Cyberspace Protection Policy of the Republic of Poland for 2011-2016 prepared by the Council of Ministers (Werner, 2014: 36).

In accordance with this document the following definition of cyberspace was adopted. 1) cyberspace – a digital space for processing and exchanging information created by information and communication systems and ICT networks, including with the connections between one another and relations with the users; 2) cyberspace of the Republic of Poland – cyberspace within the territory of the Polish State, and in locations

[7] The conceptual ISO-OSI (Open System Interconnection Reference) model is a complex standard for network communication (ISO 7498). The communication process in this model is divided into three stages called layers. There are seven layers, and their use guarantees seamless communication and data transmission in computer networks based on different topologies, while also ensuring the compatibility of the hardware used to build these systems. http://www.soisk-me.pl/klasa-iv-sieci/model-iso-osi-i-tcp-ip (accessed on 10 February 2018).
[8] NATO CCDCoE, officially the Cooperative Cyber Defence Centre of Excellence, is one of NATO Centres, based in Tallinn, Estonia. The centre conducts research and training in cybernetic security.

outside that territory, in which representatives of the Republic of Poland (diplomatic posts, military contingents) operate[9].

Defining cyberspace security became the subject of work to prepare the Doctrine of the Cybersecurity of the Republic of Poland. The following definition is provided in the document – a part of the state's cybersecurity which covers a range of organisational, legal, technical, physical, and educational ventures aimed at ensuring the uninterrupted functioning of the cyberspace of the Republic of Poland, together with its critical public and private ICT infrastructure, and the security of the information processed within that infrastructure[10]. This definition emphasises the functional aspect of cybersecurity, i.e. activities aimed to protect that space and its users.

One of the defining features of cyberspace is its network character. It is very often associated with the information revolution, and is undoubtedly connected with the rapid growth of telecommunications and the popularisation of the Internet (Szczepaniuk, 2016: 69). The network character should be considered as a constitutive attribute of cyberspace, while virtuality as a potential attribute, and as far as the communication advantages are concerned, one should not overlook hypertextuality, multimediality, and interactiveness. The combination of constitutive features and their semantic interrelations is one of the ontological aspects of cyberspace (Sienkiewicz, 2015: 92). Computer networks are a system of interrelated workstations, peripheral devices (such as printers, hard drives, scanners and workstations), and other devices. Computer networks, because of their functionality, constitute the core of all computer systems. By working within a computer network, one can share data, hardware and software, and manage all the devices connected with that network from one computer (Szczepaniuk, 2016: 70).

Seen as an illusion, virtuality creates, in relation to cyberspace, unprecedented opportunities for rendering reality. Considering cyberspace only as a virtual world creates some ambiguity. In technical terms its functioning relies fundamentally on the Internet and networks comprising computers, their components, and architecture. The space of flows is managed by certain centres, and virtual reality is created by real persons. The progress that can be seen now has made information available instantly. Space associated with certain real places has been replaced with the space of flows described by M. Castells. Formerly, space was limited geographically, whereas today it consists of various layers of unimaginable complexity (Szczepaniuk, 2016: 71).

[9] Cyberspace Protection Policy of the Republic of Poland for 2011-2016. http://bip.msw.gov.pl/bip/programy/19057,Rządowy-Program-Ochrony-Cyberprzestrzeni-RP-na-lata-2011-2016.html.
[10] The Doctrine of the Cybersecurity of the Republic of Poland. https://www.bbn.gov.pl/pl/prace-biura/publikacje/6818,Doktryna-cyberbezpieczenstwa-RP.html.

The table below sets out the development stages of cyberspace.

Table 1: An evolutionary stage model of cyberspace

Development stage	General description
Cyberspace – 0	• "The Gutenberg Galaxy" (M. McLuhan) • The development of print and the beginnings of telegraphy, telecommunications; radio, television
Cyberspace – 1	• "The Wiener Galaxy" (P. Sienkiewicz) • "The information society" (Masuda) • Cybernetic concepts of the development of social systems, the evolution of digital electronics, computer systems, satellite communications (TELSTAR), the computer network (ARPANET), "PC boom" • Artificial intelligence
Cyberspace – 2	• "The Internet Galaxy" (M. Castells) • The Internet (WWW), knowledge-based economy, globalisation
Cyberspace – 3	• "The ? Galaxy" (?) • The Internet (Web 2.0), the globalisation of the social-communications network, new forms of social behaviour • "Knowledge society" (?)

Source: (Sienkiewicz, 2012: 324).

Nowadays, cyberspace has become an environment in which contemporary society, especially its younger generation, lives and functions. Affected by globalisation, computerisation and digitisation, human activity has begun to permeate the virtual world. This has contributed to the raising of the living standards and the quality of the lives of citizens, and has increased the productiveness of entrepreneurs and the efficiency of the state. The consequence of those changes, which are becoming more and more evident, is society's dependence on cyberspace. This dependence requires the reliability of the ICT infrastructure, which in turn involves protection against potential attacks (K. Chałubińska-Jentkiewicz, 2014: 18).

Cyberspace affords huge opportunities, such as e-learning, e-administration, and telecommuting, but has its "dark side" as well. There has been an increase in the number of incidents of various kinds in the cybersecurity environment. Cyber attacks can also have a destructive influence on the state's critical infrastructure, the functioning of which is based, to a large extent, on communication and information systems (Szczepaniuk, 2016: 84).

Cyberspace protection has been one of the most addressed security-related subjects in recent years. A realisation came that an open, reliable and, above all, safe cyberspace would allow information society to function and develop globally. The raising of

awareness in this regard goes hand in hand with rapid increases in the number of computer incidents, and new categories of threats. Poland is also a target for attacks on its cyberspace. Similarly to other countries, it is faced with the challenge of working out organisational and legal changes to ensure an appropriate level of cybersecurity, and the security of the citizens who function within that space (Werner: 2014: 31).

In the field of cybersecurity there are such new terms as information security, computer-network and computer-systems security, ICT security, and cybersecurity. According to P. Potejko one can assume that information security represents a set of activities, methods, and procedures employed by competent authorities which are aimed at ensuring the integrity of collected, stored and processed information resources by protecting them against undesirable, unauthorised disclosure, modification or destruction (Potejko, 2015: 228).

The Cybersecurity Strategy of the Republic of Poland[11] defines ICT security as the resilience of communication and information systems, with a given level of trust, to counter any actions or activities which violate the accessibility, authenticity, integrity, or confidentiality of the data which are stored, shared, or processed, or related services afforded or rendered via those communication and information systems and ICT networks[12].

By comparison, the Cybersecurity Strategy of the European Union[13] defines cybersecurity as the safeguards and actions which can be used to protect the cyber domain, in both the civilian and the military fields, from those threats associated with or which might harm its interdependent networks and information infrastructure. Cybersecurity strives to preserve the availability and integrity of these networks and infrastructure, and the confidentiality of the information contained therein[14].

In the states which are involved in the development of the information society, cybersecurity is considered one of the most serious challenges in the realm of national security. It refers to the security of both the state and its individual citizens. The appropriate functioning of public administration is highly important for the maintenance of cybersecurity. The last few years have also brought a revolution in the understanding of the concept of national security as regards the subject matter. One has begun to notice

[11] The Cybersecurity Strategy of the Republic of Poland for 2017-2022. https://mc.gov.pl/aktualnosci/ strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022.
[12] Ibid.
[13] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, OJ EU C 2014.32.19.., http://www.europarl.europa.eu/meetdocs/2009_2014/ documents/ join/com_join(2013)0001_/com_join(2013)0001_pl.pdf , further "the Cybersecurity Strategy of the European Union".
[14] Ibidem, p. 3.

the significance of not only military or political aspects, but also economic, cultural, ecological, and ideological, as well as other facets. Seeing these changes, the Polish State has started to develop the National Security System, the primary focus of which is to ensure broadly understood integrated national security, in which cybersecurity occupies a very important place, covering all other aspects of social life (Chałubińska-Jentkiewicz, 2014: 20).

To recapitulate – the above analysis leads to the conclusion that each definition of cyberspace accentuates its different feature. Many of these definitions stress that cyberspace is the sum of physical components – networks, software and the information processed therein. Others additionally consider it as the sum of operations performed by the users. The increased significance of cyberspace in the functioning of numerous aspects of the state and society has led to the development of national and international cybersecurity strategies, and the further development of cybersecurity management systems.

References:

Bączek, P. (2011) *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego* (Toruń: Adam Marszałek).
Biernat, S. (1994) *Prywatyzacja zadań publicznych* (Warszawa-Kraków: PWN).
Boć, J. (ed.) (2004) *Prawo administracyjne* (Wrocław: Kolonia Limited).
Campen, S. (ed.) (1996) *The First Information War* (Washington: AFCEA).
Chałubińska–Jentkiewicz, K. (2014) *Bezpieczeństwo cyberprzestrzeni jako zadanie publiczne w systemie bezpieczeństwa narodowego RP* (Warsaw: the National Defence University of Warsaw).
Denning, D. E. (2002) *Wojna informacyjna i bezpieczeństwo informacji* (Warsaw: WNT).
Dobkowski, J. (2004) Struktura interesu publicznego a zasady rozdzielenia odpowiedzialności publicznoprawnej w Administracji, In: Ura. E (eds) *Jednostka – państwo – Administracja. Nowy wymiar* (Rzeszów: Mitel).
Grzelak, M., Liedel K (2012) Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu, *Bezpieczeństwo Narodowe*, 22/22, p. 125.
Gibson, W. (2009) *Neuromancer* (Katowice: Książnica).
Grudzewski, W. & Hejduk I. (2007) *Zarządzanie zaufaniem w organizacjach wirtualnych* (Warsaw: Difin).
Hausner, J. (2005) *Administracja publiczna* (Warsaw: PWN).
Hoffman, I. & Cseh, K. B. (2020) E-administration, cybersecurity and municipalities - the challenges of cybersecurity issues for the municipalities in Hungary, *Cybersecurity and Law*, 2(4), pp. 199-211.
Izdebski, H. & Kulesza, M. (2004) *Administracja publiczna – zagadnienia ogólne*, (Warsaw: Liber).
Jaxa Dębicka, A. (2008) *Sprawne państwo* (Warsaw: Oficyna),
Kisielnicki, J. (2008) *MIS. Systemy informatyczne zarządzania* (Warsaw: Placet).
Kitler, W. (2011) *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania*, *system* (Warsaw: the National Defence University of Warsaw).
Kłaczyński, M. & Szuster S. (2003) *Komentarz do ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej*, (Warsaw: Lex/el).

Knosala, E. (2010) *Zarys nauki administracji* (Warsaw: Oficyna).
Kocowski, T. (2012) Prywatyzacja zarządzania majątkiem publicznym, prywatyzacja majątkowa, prywatyzacja zadań publicznych i prywatyzacja wykonania zadań publicznych, In: Blicharz, J. (eds) *Prawne aspekty prywatyzacji* (Wrocław: PiEBC).
Lang, J. (1997) Zagadnienia wstępne, In: Wierzbowski, M. (eds) *Prawo administracyjne* (Warsaw: Wydawnictwo Prawnicze PWN).
Lim, S., Yoo B., Park J., Byun K. & Lee S (2012), A research on the investigation method of digital forensics for a VMware Workstation's virtual machine. *Mathematical and Computer Modelling*, 55, pp 151-160.
Lisiak-Felicka, D. & Szmit, M. (2016) *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia* (Kraków: EAS).
Martysz C., Szpor G. & Wojsyk K (2015) *Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz* (Warsaw: LEX).
Mikicka, A. K. (2012) Partnerstwo publiczno-prywatne jako prywatyzacja sensu largo zadań publicznych jednostek samorządu terytorialnego, In: Blicharz, J. (eds) *Prawne aspekty prywatyzacji* (Wrocław: PiEBC).
Monarcha–Matlak, A. (2008) *Obowiązki administracji publicznej w komunikacji elektronicznej*, (Warsaw: Oficyna).
Najda–Janoszka, M (2010) *Organizacja wirtualna. Teoria i praktyka* (Warsaw: Difin).
Ochendowski, E. (2002) *Prawo administracyjne – część ogólna* (Toruń: Zakład Poligraficzno-Wydawniczy POZKAL).
Pala, M. (2015) Wybrane aspekty bezpieczeństwa w cyberprzestrzeni, *De Securitete et Defensione O Bezpieczeństwie i Obronności*, 1, pp 113-130.
Potejko, P. (2015) Bezpieczeństwo informacyjne, In: Chałubińska-Jentkiewicz K. & Karpiuk M. *Prawo nowych technologii – wybrane zagadnienia* (Warsaw: Wolters Kluwer).
Rattray, G. T. (2004) *Wojna strategiczna w cyberprzestrzeni* (Warsaw: WNT).
Sienkiewicz, P. (2015) Ontologia cyberprzestrzeni, *Zeszyty Naukowe WWSI*, 13(9), pp 89-102.
Starościak, J. (1975) *Prawo administracyjne* (Warsaw: PWN).
Szreniawski, J (2004) *Wstęp do nauki administracji* (Lublin: Verba).
Szczepaniuk, E. (2016) *Bezpieczeństwo struktur administracyjnych w warunkach zagrożeń cyberprzestrzeni państwa* (Warsaw: the War Studies Academy).
Schmidt, P. (2012) Prywatyzacja zadań publicznych w zakresie zapewnienia dostępu do kultury, In: Blicharz, J. (eds) *Prawne aspekty prywatyzacji* (Wrocław: PiEBC).
Sienkiewicz, P. (2012) Bezpieczeństwo cyberprzestrzeni, In: Sienkiewicz P., Marszałek M. & Słota–Bohosiewicz A. (eds) *Zarzadzanie bezpieczeństwem w cyberprzestrzeni obywatela* (Warsaw: the National Defence University of Warsaw)
Stahl M (2007) Cele publiczne i zadania publiczne, In: Zimmermann J. (ed.) *Koncepcja systemu prawa administracyjnego*, (Warsaw: Wolters Kluwers).
Trajer, J., Paszek, A. & Iwan S. (2012) *Zarządzanie wiedzą* (Warsaw: PWE).
Warden, J. A. (1995) The Enemy as a System, *Airpower Journal*, 9(1), pp 41-55.
Wasilewski, J. (2013) Zarys definicyjny cyberprzestrzeni, *Przegląd Bezpieczeństwa Wewnętrznego*, 9, pp 225-234.
Werner, J. (2014) *Zagrożenia bezpieczeństwa w cyberprzestrzeni* (Warsaw: the National Defence University of Warsaw).
Władek, Z. (2013) *Organizacja i zarządzanie w administracji publicznej* (Warsaw: Difin).
Wojciechowska-Filipek, S. & Ciekanowski Z. (2016) *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki – organizacji – państwa* (Warsaw:CeDeWu).
Zimmerman, J. (2016) *Prawo administracyjne* (Warsaw: Wolters Kluwers).