Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 27/11/2026 02:12:03

Articles Studia Iuridica Lublinensia vol. 35, 1, 2026
DOI: 10.17951/sil.2026.35.1.219-232

Paweł Romaniuk
University of Warmia and Mazury in Olsztyn, Poland
ORCID: 0000-0002-7217-956X
pawel.romaniuk@uwm.edu.pl

Security of e-Administration in the System of Potential Threats in Cyberspace

Bezpieczeństwo e-administracji w systemie potencjalnych zagrożeń w cyberprzestrzeni

ABSTRACT

This paper characterizes the mechanisms of building e-administration in the circumstances of possible and probable threats that are increasingly present in cyberspace. Currently, given the broad legal and functional context, state cybersecurity has become one of the key strategic objectives in terms of adequate protection of the interests and tasks of the state. The assurance of security in cyberspace by the public authorities, whether at the central or local governance level, aims to ensure proper safeguards to benefit the community of residents, supported by appropriate control mechanisms. Due to its considerable complexity and elaborate nature, the paper focuses on selected areas of e-government security where the public sector engages with respect to public safety and potential threats in cyberspace.

Keywords: security; public administration; e-administration; threats; cyberspace; cybersecurity

INTRODUCTION

Information technology has become commonplace in the 21st century, present at every level of state functioning, and these solutions are becoming essential and indispensable. Moreover, the adaptation of the entire public administration to the changing organizational conditions associated with the application of digital

CORRESPONDENCE ADDRESS: Paweł Romaniuk, PhD, Dr. Habil., Associate Professor, University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, Department of Administrative Law and Security Sciences, Dybowskiego 13, 10-723 Olsztyn, Poland.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 27/11/2026 02:12:03

economies is so widespread that one can already speak of the progressive and inevitable digital transformation of the entire administration and, consequently, of all areas where it is active. Faced with a naturally changing functional environment, a conscious and responsible state is capable of ensuring its citizens an adequate level of security, which is one of the vital needs of every human being.[1] Obligations in the area of ensuring the security of electronic administration (e-administration) and the electronic services it provides (e-services), notably with potential threats in cyberspace in mind, rest with the bodies legitimized to act in that respect, i.e. central and local government administration agencies, which possess the appropriate scope of responsibilities, competences and sources of financing.

The main objective of this study is to assess whether adequate security of access to (and use of) broadly understood electronic services is assured, given the potential threats in cyberspace, which, as is well known, are becoming increasingly real due to the current geopolitical situation, the war in eastern Ukraine in particular. According to the adopted premise, a review of the objectives confirms that it is necessary to strengthen the security of e-administration and the electronic services it offers against various threats. The study relies on the dogmatic-legal method, involving an interpretation of selected laws and regulations as well as an analysis of doctrinal assumptions.

THE ESSENCE AND PRINCIPAL AXIOMS OF MULTIDIMENSIONAL SAFETY

The security system (and the need to ensure its proper operation) has always been an extremely important issue that has been invariably addressed, regardless of the period in which a country functions. Next to human activity, external factors – often involving various natural elements and the impact of the environment – significantly affect the level of security one seeks to ensure. It is enough to cite historical examples where the power and activity of natural elements have shown their strength, not infrequently leading to large-scale disasters.[2] Despite the fact that security science is a fairly young discipline, it should be noted that numerous approaches and attempts have already been made to define it.[3] In addition, the

[1] K. Bojarski, *Pozycja samorządu lokalnego w sferze bezpieczeństwa i porządku publicznego*, "Rocznik Samorządowy" 2012, vol. 1, pp. 22–23.

[2] Cf. B. Bonisławska, *Zadania administracji samorządowej w zakresie bezpieczeństwa publicznego – wybrane zagadnienia*, "TEKA of Political Science and International Relations" 2021, vol. 16(2), pp. 49–50.

[3] A. Furgała, *Bezpieczeństwo wewnętrzne – dylematy definicyjne w kontekście zmian ewolucyjnych i rozwoju społeczno-gospodarczego państwa*, "Przegląd Policyjny" 2020, no. 3, pp. 185–186.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 27/11/2026 02:12:03

current international situation also shows that security assumes a different meaning and becomes crucial for the protection of many spheres of state functioning.

The very notion of "security" may have diverse meanings and be tackled from different angles. It can denote public security, state security, citizen security, internal and external security, or environmental security. Security is also referred to in the Constitution of the Republic of Poland.[4] Ensuring adequate security is a matter that is duly and responsibly taken care of by state institutions.[5] Security is construed interchangeably as internal security. An interesting view is formulated by S. Sulowski, who equates security with a situation in which there is "constant readiness and activity of specific state institutions and bodies, as well as private entities, which bears on the sustained stability and integrity of the state".[6] An interesting attempt at a definition is made by E. Ura and S. Pieprzny, who find that the main distinguishing feature of security is that its effects occur within the state, whereby "internal security is a general category, comprising numerous types of security defined by the protected good or by the threat, e.g. ecological, social, fire safety".[7]

In that domain, one also encounters public security, which – in the material approach – ensures the stable functioning of all citizens in the state, spanning the entirety of social, legal, organizational and even ecological relationships that serve to mitigate the risk of threats to the functioning of the state organization and the realization of its interests, enabling its normal, unconstrained development.[8] Legal norms provide the formal guarantee of maintaining such a state of affairs, whereas competent state bodies constitute the institutional guarantee.[9] This concept denotes the security of all citizens of a state, extending beyond the security of each individual, their life, health, property, and the exercise of subjective rights, to all forms of collective life in the state organization where people coexist. That type of security presupposes the proper functioning of all public institutions, as well as social and private organizations, etc. Public security also refers to the system of protection, i.e.

[4] The tenets of security are formulated in Article 5, Article 45 (2), Article 74 (1), and Article 146 (4) (7–8) of the Constitution of the Republic of Poland of 7 April 1997 (Journal of Laws 1997, no. 78, item 483, as amended).

[5] J. Filaber, *Pojęcie bezpieczeństwa publicznego w prawie administracyjnym (wybrane uwagi)*, [in:] *Prace prawnicze, administratywistyczne i historyczne*, eds. M. Sadowski, P. Szymaniec, Wrocław 2009, pp. 246–247.

[6] See S. Sulowski, *W poszukiwaniu definicji bezpieczeństwa wewnętrznego*, "Przegląd Bezpieczeństwa Wewnętrznego" 2009, no. 1, p. 13.

[7] Internal security is discussed in detail in the monograph by E. Ura, S. Pieprzny, *Bezpieczeństwo wewnętrzne państwa*, Rzeszów 2015, p. 22.

[8] Cf. J. Kostrubiec, M. Karpiuk, D. Tyrawa, *The Status of Municipal Government in the Sphere of Ecological Security*, "Hungarian Journal of Legal Studies" 2024, vol. 65(2), pp. 169–170.

[9] See A. Misiuk, *Administracja porządku i bezpieczeństwa publicznego. Zagadnienia prawno-ustrojowe*, Warszawa 2008, p. 33.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 27/11/2026 02:12:03

a system of organizational activities and powers to apply coercive measures through specialized and duly authorized state institutions to ensure adequate protection.[10]

The public dimension of said security is not uniform. There have been interesting attempts to define the concept of public security, which may be found in the extensive literature on the subject.[11] Most authors concur that the security issue is interesting, and encompasses both the scientific and the practical dimension; however, the fact that it is characterized by indeterminacy makes it highly difficult to be precisely and comprehensively explained by means of a uniform definition.[12] An interesting position on public security is advanced by E. Ochendowski, who, following the German doctrine, argues that maintaining public safety is a state of continuous preservation of the inviolability of life, health, dignity, freedom, property, legal order and essential facilities of the state, but it also involves access to common goods, such as the public facilities which supply water or sewage collection to residents.[13] Another author, B. Jastrzębski, represents the view that public safety is a legal state in which a person has a sense of protection based largely on an efficient, effective and lawful system of public authorities, while the institutions appointed to carry out review and enforce legal norms with regard to public safety function properly and fulfil their role in the state system.[14] Moreover, skillful management of public safety covers both groups of people in social areas and representatives of the public administration community who are professionally engaged in such tasks.[15]

The above general views on security ultimately rest on the assumption that the issue in question is a state that primarily consists of protecting multiple spheres of life, including the legal order, the life and health of citizens, and national property. In addition to the aforementioned public security, there is also the matter of universal safety, which involves protecting the life and health of citizens as well as public goods from natural disasters and catastrophes. Considering the above arguments, it becomes essential to guarantee an appropriate constitutional order, where the order and functioning of the state are governed by the values and legal

[10] S. Pieprzny, *Ochrona bezpieczeństwa i porządku publicznego w prawie administracyjnym*, Rzeszów 2007, p. 22.

[11] Example definitions of public security may be found in the following studies: J. Widacki (ed.), *Ustrój i organizacja Policji w Polsce oraz jej funkcje i zadania w ochronie bezpieczeństwa i porządku (reforma Policji – część I)*, Warszawa–Kraków 1998, pp. 11–12; B. Sprengel, *Ustrój organów administracji bezpieczeństwa i porządku publicznego*, Włocławek 2004, pp. 12–13.

[12] Cf. B. Wiśniewski, S. Zalewski (ed.), *Bezpieczeństwo wewnętrzne RP w ujęciu systemowym i zadań administracji publicznej*, Bielsko-Biała 2006, pp. 29–30.

[13] E. Ochendowski, *Prawo administracyjne. Część ogólna*, Toruń 2006, p. 131.

[14] B. Jastrzębski, *O problemie prawa obywateli do bezpieczeństwa publicznego*, [in:] *Bezpieczeństwo wewnętrzne we współczesnym państwie*, eds. E. Ura, K. Rajchel, M. Pomykała, S. Pieprzny, Rzeszów 2008, pp. 16–17.

[15] M. Karpiuk, J. Kostrubiec, *Provincial Governor as a Body Responsible for Combating State Security Threats*, "Studia Iuridica Lublinensia" 2024, vol. 33(1), p. 108.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 27/11/2026 02:12:03

norms adopted in a democratic system.[16] Additionally, one must not forget about the state's ability to ensure security when it comes to protecting electronic (digital) data against unauthorized use.

THE CONCEPT OF E-GOVERNMENT FROM AN ORGANIZATIONAL AND FUNCTIONAL STANDPOINT

The idea behind e-government is to give all citizens free access to a wide range of public services via the internet. The development and use of electronic services is becoming an increasingly popular form of communication between public institutions and citizens. The main task facing modern public administration today is the provision of services. It is apparent that electronic administration (e-administration) is becoming increasingly widespread and popular. Examples of e-services include submitting tax returns or applying for a new ID card online. These are just a few examples of services that are increasingly often provided by means of electronic communication. The widespread use and availability of electronic systems to citizens is intended to improve interaction with administrative authorities and speed up the procedures concerned with formal affairs, which is particularly important at the local government level. It is worth noting that, in a narrow sense, e-administration means the use of information and communication technologies (ICT) in the process of providing public services, while in a broad sense, it assumes a transformative character, being associated with the inevitable technological progress and the need to introduce numerous changes in the public sector.[17] In the subjective approach, e-administration represents an integral part of the so-called "digital governance ecosystem", which encompasses various public entities, entrepreneurs, NGOs, civil governance bodies, and individuals who actively promote and disseminate available databases and public services through mutual interaction.[18]

The use of various types of e-services is largely motivated by several factors, such as saving time, expanding the scope and variety of services provided, convenience, overcoming spatial and temporal barriers, and achieving financial benefits.[19]

---

[16] Cf. W. Kitler, *Bezpieczeństwo wewnętrzne w świetle współczesnych wyzwań teorii i praktyki problemu*, "Wiedza Obronna" 2023, vol. 282(1), pp. 130–132.

[17] J. Blicharz, L. Zacharko, *Europejska sieć ds. administracji publicznej*, [in:] *Wzorce i zasady działania współczesnej administracji publicznej*, eds. B. Jaworska-Dębska, P. Kledzik, Warszawa 2020, pp. 821–824.

[18] See the position outlined in E. Barcevičius, G. Cibaitė, C. Codagnone, V. Gineikytė, L. Klimavičiūtė, G. Liva, L. Matulevič, G. Misuraca, I. Vanini, *Exploring Digital Government Transformation in the EU – Analysis of the State of the Art and Review of Literatur*e, Luxembourg 2019, p. 13.

[19] See more in A. Dąbrowska, M. Janoś-Kresło, A. Wódkowski, *E-usługi a społeczeństwo informacyjne*, Warszawa 2009, pp. 137–138.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 27/11/2026 02:12:03

Furthermore, the main asset which makes e-administration so significant is its unlimited availability. Information conveyed to all recipients electronically, through e.g. the Public Information Bulletin platform, involves an unlimited time frame, where information is available to every potential recipient 24 hours a day, 7 days a week. Such a direction of change in access to source data is an important, though not the only, attribute characterizing contemporary e-administration. Target-oriented changes also apply to the very possibility of diversifying and facilitating the manner of handling most official matters by means of IT tools. Naturally, one cannot overlook that the widespread use of this form of public service delivery requires several additional factors. For example, there must be increased public awareness that translates into the use of this form to contact various offices, as well as widespread education about the technological means of handling such matters.

An interesting assessment is suggested by Z. Stempnakowski, who aptly notes that electronic offices are treated as "up-to-date" products that meet the expectations of citizens and ensure faster and often cheaper handling of public affairs. The author also maintains that a contemporary public administration that changes and takes advantage of electronic communication becomes more competitive and adapts its standards to the new possibilities for the public sector, which result from the natural and inevitable globalization of the modern world.[20] However, it is important to remember that changes in the functioning of public administration are a necessity today, and everyone must be prepared for the naturally changing form of the services offered. In such organizational circumstances, e-administration is expected to be an extremely flexible, open and largely understandable and friendly mechanism, ensuring the cooperation of administrative staff in order to handle customers' affairs and meet their essential needs. The effort to modify contemporary administration must undoubtedly be supported by multiple ICT systems that link compatible electronic document circulation systems with other public registers that may as yet be unintegrated.[21]

Technological changes in the operation of public administration are becoming a reality. Therefore, it would be legitimate to cite several important elements mentioned by M. Ganczar, which highlight the need to introduce solutions in the field of e-administration and e-services, even though many are already being implemented,[22] i.e.:

---

[20] Z. Stempnakowski, *Administracja elektroniczna*, [in:] *Społeczeństwo informacyjne – problemy rozwoju*, ed. A. Szewczyk, Warszawa 2007, pp. 57–58.

[21] J. Janowski, *Technologia informacyjna dla prawników i administratywistów. Szanse i zagrożenia elektronicznego przetwarzania danych w obrocie prawnym i działaniu administracji*, Warszawa 2009, pp. 53–54.

[22] M. Ganczar, *Informatyzacja administracji publicznej. Nowa jakość usług publicznych dla obywateli i przedsiębiorców*, Warszawa 2009, pp. 36–39.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 27/11/2026 02:12:03

- implementation of a proper telecommunications infrastructure, combined with the implementation of innovative technological projects and the implementation of relations connecting the public sector with the organizational environment by means of modern technologies;
- utilizing human capital in administration, guaranteeing that the staff has the sufficient skillset to use ICT services;
- ensuring changes in the system of managing personnel and tasks, as both require being adapted to the new work practice;
- building an e-business atmosphere, which is becoming necessary in order to create a modern environment, including an adequate legal framework;
- conducting regular, modular and strictly thematic training courses aimed at achieving full readiness to use new information and communication tools;
- reducing the resistance of public administration personnel that results from awareness building and the necessity of work changes, using modern technologies for this purpose.

It should also be noted that, when using financing services provided by means of electronic communication, it is vital to offer potential recipients document management systems of adequate quality.[23] The role of such systems is precisely the ability to properly acquire, process and store documents in digital form. The actions taken should allow for the strategy of each public institution, including its document content management system. Each of these strategies should, in particular, be concerned with the registration of documents received by offices in paper and electronic form, the correct classification of such documents, document circulation management, control of authorizations granted within the framework of e-service management, as well as document archiving.[24]

The so-called trusted profile – increasingly popular and used by Poles – plays an important role in the process of providing services by electronic means. The trusted profile is a free platform whose main purpose is to ensure an electronic citizen ID in various electronic administration systems. The trusted profile is also used to submit a signature that links the holder to a specific addressee. For example, using this tool, one can file an application, request, appeal or complaint. The advantage of this solution is that there is no need to print a document, sign it by hand, and scan it. The electronic signature is just as valid as its handwritten equivalent. Therefore, the profile includes data that clearly validates the user of such an account and indicates the precise time when such identification was performed.[25]

[23] Cf. M. Jachowicz, M. Kotulski, *Forma dokumentu elektronicznego w działalności administracji publicznej*, Warszawa 2012, pp. 46–47.

[24] S. Wrycza, *Informatyka ekonomiczna*, Warszawa 2010, pp. 434–435.

[25] K. Lorenz, *Podpis zaufany w rozwoju e-administracji*, "Studia Informatica Pomerania" 2017, no. 3, p. 27.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 27/11/2026 02:12:03

E-ADMINISTRATION AND THE POTENTIAL THREATS IN CYBERSPACE

As regards threats in cyberspace that may affect the provision of electronic services by public administration, it is necessary to define what cyberspace is. It should be noted that the concept began to appear as early as the 1980s. It may also be worthwhile to mention William Gibson's assessment, who saw cyberspace as a virtual reality in which the world consists of digital networks in the form of battlefields where global corporations clash, while new economic and cultural boundaries are at stake.[26] Nowadays, this term describes the multiple virtual connections that have been created within the broadly understood telecommunications infrastructure.[27] There are also those for whom cyberspace means all connections that link human activity with information and communication technology.[28] It should also be noted that, in addition to cyberspace, issues related to cyberterrorism are becoming important. According to one of the Polish definitions of cyberterrorism, it is an action that blocks, distorts or destroys the information processed, stored and transmitted by means of ICT systems, as well as activities affecting the proper operation of systems.[29] This term denotes the use of ICT systems for disinformation, where the target of the attack is not the system but the processed information.

Provisions contained in the National Cybersecurity System Act[30] constitute an important legal basis relating to cyberspace. The chief purpose of that legal act is to set out how the national cybersecurity system is organized and how it is supposed to function. It also specifies the methods of supervision and control within the scope of application of the act.[31] Therefore, it may be concluded that the cyberspace in question is a network connecting computer systems that encompass all entities – including their software and data – which use appropriate methods to transfer them. In a broader sense, cyberspace may encompass interconnected internet systems, communications, transport, energy, gas, water, infrastructure, healthcare, and many other ICT services that operate online.[32]

---

[26] See M. Nowak, *Cybernetyczne przestępstwa. Definicje i przepisy prawne*, Poznań 2010, p. 5.

[27] Cf. M. Madej, *Rewolucja informatyczna*, [in:] *Bezpieczeństwo teleinformatyczne państwa*, eds. M. Madej, M. Terlikowski, Warszawa 2009, pp. 28–29.

[28] Such a view is expressed by A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego*, Warszawa 2003, pp. 36–38.

[29] P. Jankowski, *Cyberterroryzm jako współczesne zagrożenie dla administracji publicznej*, "Młody Jurysta" 2018, no. 4, pp. 17–18.

[30] Act of 5 July 2018 on the national cybersecurity system (consolidated text, Journal of Laws 2024, item 1077, as amended).

[31] K. Kupińska, *Zagrożenia cybernetyczne w funkcjonowaniu administracji publicznej powiatu jarosławskiego*, "Współczesne Problemy Zarządzania" 2022, vol. 10(1), p. 31.

[32] P. Tekielska, Ł. Czekaj, *Działania służb w UE realizujących zadania na rzecz bezpieczeństwa cybernetycznego*, [in:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, ed. M. Górka, Warszawa 2014, pp. 161–163.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 27/11/2026 02:12:03

With respect to cyberspace, one should also mention the cybersecurity of digital services provided by public institutions, which is determined by the security of IT systems. In this respect, it is important that digital service providers have the means to protect the security of their IT systems (information and communication systems with the electronic data they process) against numerous threats using a holistic approach. In this case, the risk management system must be based on risk assessment and analysis, taking into account ICT system failures, human factors, errors, undesirable actions and natural phenomena.[33]

The state of information security in cyberspace may only be achieved if several key conditions are met, including, in particular:

- absence of potential threats to the state's strategic resources;
- public administration bodies make decisions based on reliable, up-to-date and verified information;
- the flow of information between public authorities is secure;
- adequate control is maintained over ICT networks that constitute the critical infrastructure of the state;
- assured protection of classified information and citizens' personal data, as well as the inviolability of their right to privacy and access to public information.

Cyberspace is, therefore, becoming an environment with both informational and defensive features, where information introduced into a computer's memory may serve to combat, e.g. espionage, various forms of ordinary crime (bank account theft, extortion, fraud) and, unfortunately, increasingly frequent terrorism.[34] In the doctrine, several dozen types of hacking tools have already been developed to attack IT systems.[35] Another, but comparable assessment of threats in cyberspace is advanced by P. Lubiewski, according to whom threats originate with persons acting in groups or taking individual action. In the catalogue of threats, he mentions, in particular, the disclosure of classified information, violation of citizens' rights, cyber intrusion or trespassing, sabotage and computer fraud, manipulation

[33] More broadly in M. Karpiuk, *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, "Studia Iuridica Lublinensia" 2023, vol. 32(2), pp. 193–194.

[34] J.P. Kwaśniewski, *E-administracja na tle zagrożeń w cyberprzestrzeni*, [in:] *XVI Interdyscyplinarna Konferencja Naukowa TYGIEL 2024 „Interdyscyplinarność kluczem do rozwoju*", eds. P. Pomajda, K. Maciąg, Lublin 2024, p. 213.

[35] E. Lichocki (*Model systemu zarządzania w warunkach zagrożeń dla bezpieczeństwa informacyjnego*, Warszawa 2009, pp. 61–63) lists various types of hacking activities, which include: viruses, worms (malware or malicious software), trojans, false authentication, unauthorized file copying, unauthorized access to information, theft involving takeover of system resources, installation of malicious components in a computer in the form of chips that generate hardware defects, interception of transmissions, i.e. gaining access to information sent between computers, surveillance which involves tracking network traffic.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 27/11/2026 02:12:03

of information, development of uncontrolled modern technologies, asymmetric threats, espionage and cyberterrorism.[36]

The use of modern computer technology in public administration increases the potential risk of losing important data, unauthorized access to data and system failures. Contemporary ICTs are developing very dynamically, which is why new security measures and protection systems should be introduced constantly. An interdisciplinary approach to digital information security and its comprehensive implementation is becoming essential. It should also be noted that humans are one of the weakest links in the IT system. Unfortunately, human error can be much more prevalent than IT system failure, whereby it mostly affects systems that are connected to a decentralized network, such as the internet.[37]

Moreover, the successful implementation of new legal and functional solutions in the development of electronic services for the proper operation of public administration hinges on many factors that are closely related to technological, economic, cultural and, consequently, human aspects.[38] The above activities may assume a variety of forms. They may be undertaken by service providers or be present in the external sphere, which, in turn, strictly involves the users of services themselves. The use of modern technologies in public administration should be oriented towards introducing necessary management changes, thus emphasizing the use of modern tools, all the while taking potential risks into account. Proposals *de lege ferenda* in the field of electronic services are aimed at building transparency of the tasks performed by the administration, as well as improving their effectiveness and efficiency while building good relations with citizens and strengthening their trust in the sector. Solutions promoting the development of e-administration in the broad sense should be deployed at all tiers of administration while responding to social needs and expectations, thus guaranteeing effective and efficient administration of digital resources.[39]

CONCLUSIONS

In conclusion, it should be noted that the electronic services market in Poland is developing very dynamically, expanding to further areas. Moreover, most of the services available online are becoming increasingly accessible and user-friendly.

[36] P. Lubiewski, *Szczególna dynamika zmian współczesnych zagrożeń w sferze bezpieczeństwa publicznego na przykładzie cyberprzestrzeni*, "Zeszyty Naukowe SGSP" 2020, vol. 76(4), pp. 38–39.

[37] I. Kin-Dittmann, *Szanse i zagrożenia rozwoju polskiej e-administracji*, "Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2010, no. 10, p. 86.

[38] Cf. M.A. Shareef, V. Kumar, U. Kumar, Y.K. Dwivedi, *e-Government Adoption Model (GAM): Differing Service Maturity Levels*, "Government Information Quarterly" 2011, vol. 28(1), pp. 17–33.

[39] P. Romaniuk, *Szanse i zagrożenia dla administracji publicznej w świadczeniu usług drogą elektroniczną*, "Studia Prawnoustrojowe" 2022, no. 58, pp. 450–451.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 27/11/2026 02:12:03

Thanks to innovative forms of accessing the internet, including mobile technologies, the number of people using the internet is increasing every year, and new technological services are being introduced. Modern e-services provided by public administration should focus primarily on mobility, community, originality, individuality and ease of use. The new possibilities of such electronic communication ensure greater access to it and increased demand for such services. The successive implementation of innovative technological solutions must go hand-in-hand with the provision of appropriate IT, technical and organizational conditions to enable the functioning of multiple ICT systems and public registers.

It follows from the assessments presented in this study that e-administration is making visible progress as far as various threats in cyberspace are concerned. The introduction of new legal solutions, training, financing of software purchases, and the creation of secure internet portals are just a few of the measures taken by the state to increase citizens' confidence in e-administration as well as raise public awareness that it may be securely used. This does not change the fact that both the computers of individual users and servers within IT systems should be constantly secured. In order to detect malware, it is necessary to install anti-virus software, while backup copies of data need to be made as part of IT system risk prevention. Even though numerous technical solutions are used to foster a sense of security in cyberspace, the common sense of users and their knowledge of potential dangers are also extremely important. Given the natural and inevitable development of e-administration, security training and awareness-raising are particularly needed. In consequence, both citizens and public administration personnel will be more aware of the risks, grow familiar with the principles of security policies, and possess sufficient knowledge of how to counter potential threats in cyberspace.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 27/11/2026 02:12:03

REFERENCES

Literature

Barcevičius E., Cibaitė G., Codagnone C., Gineikytė V., Klimavičiūtė L., Liva G., Matulevič L., Misuraca G., Vanini I., *Exploring Digital Government Transformation in the EU – Analysis of the State of the Art and Review of Literatur*e, Luxembourg 2019.

Blicharz J., Zacharko L., *Europejska sieć ds. administracji publicznej*, [in:] *Wzorce i zasady działania współczesnej administracji publicznej*, eds. B. Jaworska-Dębska, P. Kledzik, Warszawa 2020.

Bojarski K., *Pozycja samorządu lokalnego w sferze bezpieczeństwa i porządku publicznego*, "Rocznik Samorządowy" 2012, vol. 1.

Bonisławska B., *Zadania administracji samorządowej w zakresie bezpieczeństwa publicznego – wybrane zagadnienia*, "TEKA of Political Science and International Relations" 2021, vol. 16(2). **DOI: https://doi.org/10.17951/teka.2021.16.2.49-62**

Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego*, Warszawa 2003.

Dąbrowska A., Janoś-Kresło M., Wódkowski A., *E-usługi a społeczeństwo informacyjne*, Warszawa 2009.

Filaber J., *Pojęcie bezpieczeństwa publicznego w prawie administracyjnym (wybrane uwagi)*, [in:] *Prace prawnicze, administratywistyczne i historyczne*, eds. M. Sadowski, P. Szymaniec, Wrocław 2009.

Furgała A., *Bezpieczeństwo wewnętrzne – dylematy definicyjne w kontekście zmian ewolucyjnych i rozwoju społeczno-gospodarczego państwa*, "Przegląd Policyjny" 2020, no. 3.

Ganczar M., *Informatyzacja administracji publicznej. Nowa jakość usług publicznych dla obywateli i przedsiębiorców*, Warszawa 2009.

Jachowicz M., Kotulski M., *Forma dokumentu elektronicznego w działalności administracji publicznej*, Warszawa 2012.

Jankowski P., *Cyberterroryzm jako współczesne zagrożenie dla administracji publicznej*, "Młody Jurysta" 2018, no. 4. **DOI: https://doi.org/10.21697/mj.2018.4.03**

Janowski J., *Technologia informacyjna dla prawników i administratywistów. Szanse i zagrożenia elektronicznego przetwarzania danych w obrocie prawnym i działaniu administracji*, Warszawa 2009.

Jastrzębski B., *O problemie prawa obywateli do bezpieczeństwa publicznego*, [in:] *Bezpieczeństwo wewnętrzne we współczesnym państwie*, eds. E. Ura, K. Rajchel, M. Pomykała, S. Pieprzny, Rzeszów 2008.

Karpiuk M., *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, "Studia Iuridica Lublinensia" 2023, vol. 32(2). **DOI: https://doi.org/10.17951/sil.2023.32.2.189-201**

Karpiuk M., Kostrubiec J., *Provincial Governor as a Body Responsible for Combating State Security Threats*, "Studia Iuridica Lublinensia" 2024, vol. 33(1). **DOI: https://doi.org/10.17951/sil.2024.33.1.107-122**

Kin-Dittmann I., *Szanse i zagrożenia rozwoju polskiej e-administracji*, "Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2010, no. 10.

Kitler W., *Bezpieczeństwo wewnętrzne w świetle współczesnych wyzwań teorii i praktyki problemu*, "Wiedza Obronna" 2023, vol. 282(1). **DOI: https://doi.org/10.34752/2023-f282**

Kostrubiec J., Karpiuk M., Tyrawa D., *The Status of Municipal Government in the Sphere of Ecological Security*, "Hungarian Journal of Legal Studies" 2024, vol. 65(2). **DOI: https://doi.org/10.1556/2052.2024.00510**

Kupińska K., *Zagrożenia cybernetyczne w funkcjonowaniu administracji publicznej powiatu jarosławskiego*, "Współczesne Problemy Zarządzania" 2022, vol. 10(1). **DOI: https://doi.org/10.52934/wpz.173**

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 27/11/2026 02:12:03

Kwaśniewski J.P., *E-administracja na tle zagrożeń w cyberprzestrzeni*, [in:] *XVI Interdyscyplinarna Konferencja Naukowa TYGIEL 2024 „Interdyscyplinarność kluczem do rozwoju*", eds. P. Pomajda, K. Maciąg, Lublin 2024.

Lichocki E., *Model systemu zarządzania w warunkach zagrożeń dla bezpieczeństwa informacyjnego*, Warszawa 2009.

Lorenz K., *Podpis zaufany w rozwoju e-administracji*, "Studia Informatica Pomerania" 2017, no. 3. **DOI: https://doi.org/10.18276/si.2017.45-03**

Lubiewski P., *Szczególna dynamika zmian współczesnych zagrożeń w sferze bezpieczeństwa publicznego na przykładzie cyberprzestrzeni*, "Zeszyty Naukowe SGSP" 2020, vol. 76(4). **DOI: https://doi.org/10.5604/01.3001.0014.5978**

Madej M., *Rewolucja informatyczna*, [in:] *Bezpieczeństwo teleinformatyczne państwa*, eds. M. Madej, M. Terlikowski, Warszawa 2009.

Misiuk A., *Administracja porządku i bezpieczeństwa publicznego. Zagadnienia prawno-ustrojowe*, Warszawa 2008.

Nowak M., *Cybernetyczne przestępstwa. Definicje i przepisy prawne*, Poznań 2010.

Ochendowski E., *Prawo administracyjne. Część ogólna*, Toruń 2006.

Pieprzny S., *Ochrona bezpieczeństwa i porządku publicznego w prawie administracyjnym*, Rzeszów 2007.

Romaniuk P., *Szanse i zagrożenia dla administracji publicznej w świadczeniu usług drogą elektroniczną*, "Studia Prawnoustrojowe" 2022, no. 58. **DOI: https://doi.org/10.31648/sp.8055**

Shareef M.A., Kumar V., Kumar U., Dwivedi Y.K., *e-Government Adoption Model (GAM): Differing Service Maturity Levels*, "Government Information Quarterly" 2011, vol. 28(1). **DOI: https://doi.org/10.1016/j.giq.2010.05.006**

Sprengel B., *Ustrój organów administracji bezpieczeństwa i porządku publicznego*, Włocławek 2004.

Stempnakowski Z., *Administracja elektroniczna*, [in:] *Społeczeństwo informacyjne – problemy rozwoju*, ed. A. Szewczyk, Warszawa 2007.

Sulowski S., *W poszukiwaniu definicji bezpieczeństwa wewnętrznego*, "Przegląd Bezpieczeństwa Wewnętrznego" 2009, no. 1.

Tekielska P., Czekaj Ł., *Działania służb w UE realizujących zadania na rzecz bezpieczeństwa cybernetycznego*, [in:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, ed. M. Górka, Warszawa 2014.

Ura E., Pieprzny S., *Bezpieczeństwo wewnętrzne państwa*, Rzeszów 2015.

Widacki J. (ed.), *Ustrój i organizacja Policji w Polsce oraz jej funkcje i zadania w ochronie bezpieczeństwa i porządku (reforma Policji – część I)*, Warszawa–Kraków 1998.

Wiśniewski B., Zalewski S. (ed.), *Bezpieczeństwo wewnętrzne RP w ujęciu systemowym i zadań administracji publicznej*, Bielsko-Biała 2006.

Wrycza S., *Informatyka ekonomiczna*, Warszawa 2010.

Legal acts

Act of 5 July 2018 on the national cybersecurity system (consolidated text, Journal of Laws 2024, item 1077, as amended).

Constitution of the Republic of Poland of 7 April 1997 (Journal of Laws 1997, no. 78, item 483, as amended).

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 27/11/2026 02:12:03

ABSTRAKT

W artykule scharakteryzowano mechanizmy budowania e-administracji w warunkach możliwych i prawdopodobnych zagrożeń, coraz częściej obecnych w cyberprzestrzeni. Przedmiotowe cyberbezpieczeństwo państwa staje się we współczesnych czasach i prawno-funkcjonalnych uwarunkowaniach jednym z kluczowych celów strategicznych w obszarze należytego zabezpieczenia interesów i zadań państwa. Gwarancja bezpieczeństwa w cyberprzestrzeni, należąca do władz publicznych, zarówno rządowych, jak i samorządowych, zmierza do zapewnienia właściwej ochrony społeczności mieszkańców, wspieranych odpowiednimi mechanizmami kontrolnymi. W artykule przybliżono wybrane, z uwagi na ich dość złożony i rozbudowany charakter, obszary z zakresu bezpieczeństwa funkcjonowania e-administracji, które wdrażane są przez sektor publiczny w obszarze bezpieczeństwa publicznego i potencjalnych zagrożeń w cyberprzestrzeni.

Słowa kluczowe: bezpieczeństwo; administracja publiczna; e-administracja; zagrożenia; cyberprzestrzeń; cyberbezpieczeństwo

UMCS