DOI: 10.14746/r.2017.2.3

Martyna Kinga CZYŻ

Adam Mickiewicz University in Poznań

# Information and communications security as a new challenge faced by Poland in 2007–2017

**Abstract:** The aim of the article is to present the challenges faced by Poland in developing its ICT security strategy. The author attempts to define ICT security and its scope and identify the threats to Poland over the last decade. Rapid technological progress quickly renders any approach obsolete. Therefore, a state wishing to provide its citizens with adequate protection is forced to adopt proper measures. In view of this goal, the author discusses the efforts made by the Polish government to achieve its strategic cyberspace security objectives. She demonstrates that the future ICT security of Poland depends largely on developing a single all-encompassing legislative instrument.

**Key words:** cybersecurity, ICT, security risks

ICT (Information and Communications Technology) security has been brought to the forefront by rapid technological advances which fueled an ICT revolution and transformed every sphere of human life. Among the key resulting challenges, Marcin Terlikowski (2011) points to changes in business environments, interpersonal communications and leisure pursuits as well as an evolution of the mass culture.

Marshall McLuhan notes that "the new electronic interdependence recreates the world in the image of a global village" (McLuhan, 2011, p. 36). However, greater interdependence brings with it not only new opportunities but also new threats, one of the most serious of which is growing dependence on ICT systems (Skrzypczak, 2011, p. 51). Being relatively new, threats of this kind remain fairly unknown, posing a wide range of challenges for members of the international community, including Poland.

As the issue is relatively new, only a few studies on the topic are available in Polish scholarly literature. A mere handful of Polish-language articles related directly to ICT security have been published to date. The most prominent of them are *Bezpieczeństwo teleinformatyczne państwa* [State

cybersecurity] by Marek Madej and Marcin Terlikowski, *Terroryzm i cyberterroryzm jako największe wyzwanie bezpieczeństwa współczesnego państwa* [Terrorism and cyberterrorism as the biggest security challenge to today's states] by Tomasz Aleksandrowicz, Agnieszka Bógdał-Brzezińska, Jarosław Gryz, Izabela Oleksiewicz and Grzegorz Ostasz, and *Terroryzm i bezpieczeństwo fizyczne i teleinformatyczne informacji niejawnych* [Terrorism and the physical and ICT security of classified information] by Mariusz Jabłoński. The issues referred to in their titles receive the most attention in research on new post-Cold-War challenges and studies by independent think tanks, such as the Casimir Pulaski Foundation and the Kosciuszko Institute.

The aim of this article is to examine current threats to ICT security and the challenges they pose to Poland. The paper covers the period from 2007 to 2017, which saw a series of events that contributed to increasing the significance of ICT security in general state security strategies.

The author attempts to define and identify: (i) the meaning of ICT security, (ii) the risks it poses, and (iii) Poland's response to such risks.

The main challenge in addressing the above issues lies in the lack of a uniform cyberspace protection program in Poland. The deficiency results from constant advances in technology and the continuous evolution of threats, which quickly renders any established approach obsolete.

## ICT security – the concept

ICT security is commonly defined as "ensuring access to and the integrity and confidentiality of information" (Terlikowski, 2011). Under the approach, data integrity refers chiefly to the certainty that no data gets modified without the consent and knowledge of its user or administrator. Confidentiality, in its turn, denotes the certainty that no data is acquired by unauthorized parties.

Simply put, ICT security can be defined as all issues related to the management of risks associated with the use of computers, with security being conditional upon the proper operation of all ICT systems used to process classified information and/or systems belonging to networks used to control critical state infrastructure (Terlikowski, 2011).

To define security solely in terms of the technical operating parameters of systems while ignoring the broader context of their functioning is to take a very narrow approach. Notably, this is only one of many pos-

sible viewpoints on the issue, as the concept itself is highly ambiguous and multifaceted.

ICT security can be examined on many levels. Its analysis may begin with individual computer users, which is the lowest level. In a much broader approach, research extends to enterprises and institutions that rely on computer systems to run their processes. It may go even further to the state level or that of the international community at large (Madej, Terlikowski, 2009, p. 4).

The scope of ICT security varies with each such level. Each level is exposed to a unique set of risks, which vary in their extent, the severity of security breach impacts, and the arsenals of measures and methods deployed to ensure adequate security (ibid.). Due precisely to the multifaceted nature of the issue, it is absolutely vital that the significance and character of the threats faced by the state at any particular time be properly identified and assessed.

## ICT security risks faced by the state

All fundamental ICT security risks enumerated in literature result from deliberate efforts to, *inter alia*, develop and disseminate malicious software and/or engage in the unauthorized remote manipulation of systems (Terlikowski, 2011).

The severity of such risks at the national level depends on the perpetrators and their intent (Terlikowski, 2011). This divides risks into two main categories of economically driven and politically motivated.

The former are linked to criminal activities in cyberspace, known as cybercrime. The American Internet Crime Complaint Center defines cybercrime as "online fraud in any of its multiple manifestations such as the theft of intellectual property rights, computer intrusion, economic espionage, online extortion, international money laundering, identity theft and a growing number of crimes facilitated by the Internet" (Lakomy, 2013, p. 130).

In recent years, threats of this kind have also been observed in Poland. The media increasingly report on fraudsters targeting bank account holders. In a recent highly publicized confidence scam, e-mails containing a link to a fake login page were sent to Mbank customers (TVN24, 2016). Another example are recent reports on the malfunction of the online banking system of BGŻ BNP Paribas (TVN24, 2016a). There is also

a growing risk of identity theft and the leakage of critical personal information. Especially upsetting to the general public was the recent suspicious data migration from the PESEL (personal identification number) system (TVN24, 2016b).

It has nevertheless been noted that the majority of such threats arise at the lowest level. As remarked by Terlikowski, "cybercriminals have neither the capacity nor the resolve to target the state or its institutions" (Terlikowski, 2011). The above notwithstanding, threats of this kind must be combated relentlessly by legislative means and/or through awareness raising campaigns.

The risks that are more critical for the state are the ones that are motivated politically. One of the most severe of them is cyberterrorism (Aleksandrowicz, Bógdał-Brzezińska, Gryz, Oleksiewicz, Ostasz, 2016, p. 10). Its key feature is "the intent, that is characteristic of terrorism, to inflict maximum damage on e.g. critical state infrastructure with a view to undermining the sense of safety in the general public" (Lakomy, 2013, p. 131). The digital revolution has exposed states to attacks by hostile organizations that have acquired the prerequisite know-how. The distinctive low cost of such operations, their unpredictability and locations have the potential to render states vulnerable to such attacks (Aleksandrowicz, Bógdał-Brzezińska, Gryz, Oleksiewicz, Ostasz, 2016, pp. 76–77). One game-changing event that dramatically altered the perception of such risks was the cyberattack on Estonia (NBC News, 2009).

During the attack, electronic devices were flooded with streams of random data, which overloaded and effectively crashed the entire system leading to the denial of service (DDoS). The resulting web paralysis brought chaos into the lives of thousands of Estonians. The impact was particularly severe due to the state's heavy dependence on web-based services as nearly all of its administration operated online. In 2007, Estonia adopted an e-voting system to accommodate its election in that year. 86% of the population relied on electronic banking (Kozłowski, 2014, p. 238). Although the attack inflicted no significant physical damage, it is considered a watershed. Being the first onslaught on such an enormous scale, it exposed defense weaknesses, laying bare the growing peril of cyberspace security lagging behind the rising activity of criminals prepared to take on even entire states.

It is vital to realize that the threat is real and that, just as any other state, Poland may be struck at any time. For now, the country has only sustained small-scale attacks on individual institutions and enterprises.

A DDoS was experienced by, among others, the Polish national airline LOT, whose aircraft were effectively grounded in June 2015 (Reuters, 2015). However, this was not an isolated incident and, in fact, the likelihood that others will follow is rising. According to the Polish Ministry of Treasury, a significantly greater risk is now being faced by small and medium-sized enterprises (SMEs). Public administration and critical state infrastructure are particularly vulnerable. The risk may be additionally aggravated since the Ukrainian conflict extended into cyberspace (Ministry of Treasury, 2015). This particular danger has been confirmed by the incident of August 2014 in which the Polish embassy in Ukraine became the target of an attack, presumably by Russian hackers ("Financial Times", 2014). One must prepare to see the kinds of attacks currently observed in individual organizations threaten entire states in the near future.

Another form of politically-motivated malicious activity is cyber espionage. Lakomy (2013, p. 131) defines it as "an attempt to obtain classified information in cyberspace." The threat has been growing rapidly and steadily since 2008. New acts of electronic espionage on a massive scale are being discovered in the US, Norway, France and Germany, carried out most likely by Chinese hackers (Terlikowski, 2011). Cyber espionage may pose a real threat to Poland. The above-mentioned report by the Ministry of Treasury shows that domestic enterprises may increasingly be exposed to ATP (advanced persistent threat) attacks aimed mainly at harvesting classified information. In 2014, the number of such attacks is said to have grown by 41% on the previous years (Ministry of Treasury, 2015). It is also projected that such attacks will increasingly be perpetrated by states. Mirosław Maj, President of the Safe Cyberspace Foundation, recognizes that "hacktivist operations, whose main effect is to spread propaganda, will soon be replaced by state-sponsored cyber espionage, with all of its consequences" (Ministry of Treasury, 2015). Joanna Świątkowska adds that Poland finds the situation in Ukraine to be of particular relevance (Ministry of Treasury, 2015).

Needless to say, the above list is non-exhaustive and constantly growing. Some of the new items added to the list include manipulation of public opinion or the use of cyberspace as a "new theater of war" (Lakomy, 2013, p. 131).

Regardless of how the list is compiled, one should bear in mind that all aspects of ICT security stated therein apply to Poland just as much as they do to any other states that are equally or more developed. Due to their close integration with international systems, including those of such organizations as the EU and NATO, Polish IT networks are today and/or

may become in the future the targets of various types of attacks (Ministry of Treasury, 2015, Terlikowski, 2011). This makes it all the more imperative to avert the threats.

## Measures to enhance ICT security

A great deal has been done in recent years to protect the Polish cyberspace. A major effort has been made by the Polish Internal Security Agency (ABW), whose statutory responsibilities include protecting the ICT systems used to process classified information (Protection of Classified Information Act, 2010, Art. 10).

To that end, the Internal Security Agency focuses mainly on:

- Managing ICT protection and arranging for IT security training;
- Obtaining ICT security accreditation for ICT systems intended to process classified national information;
- Obtaining ICT security accreditation for ICT systems intended to process classified international information;
- Selecting appropriate electromagnetic protection measures;
- Certifying electromagnetic protection measures, ICT security tools and cryptographic devices and tools (ABW, 2010).

Up until recently, deficient cyber security legislation posed serious challenges (Gapiński, 2016, p. 1). However, significant improvements have been made. As a first step to remedy the problem, the Polish lawmakers adopted the term "cyberspace," which they defined as "space used to process and exchange information generated by such ICT systems as are referred to in Art. 3.3 of the February 17, 2005 Act on the digitization of public bodies (Journal of Laws of 2014, Item 1114), as well as any mutual links among such bodies and their relations with users (Journal of Laws of 2002, No. 156, Item 1301)." The 2004 amendment of the Penal Code, aimed at harmonizing Polish criminal law with European requirements (subsequently amended in 2008), added new types of offenses to the Polish substantive criminal law to ensure that computer crime is penalized more effectively (Aleksandrowicz, Bógdał-Brzezińska, Gryz, Oleksiewicz, Ostasz, 2016, pp. 96–110).

In the subsequent years, the authorities sustained their effort towards adopting a uniform cyberstrategy and establishing a well-functioning cyber security system. The most important manifestations of this type of activity include:

- The Act of April 26, 2007 on crisis management, which clearly defines critical infrastructure, described as "any systems and their functionally linked components, including buildings and other structures, devices, installations and networks, services that are of critical importance for state and public security and used to ensure the unimpeded operation of public administration bodies, institutions and businesses" as well as the systems used by such organizations (Crisis Management Act, 2007, Art. 3). The key sectors of vital importance for state security are deemed to be the energy, communications, finance, food and water supply, health protection, transport, rescue, systems ensuring the continuous operation of public administration and hazardous substance infrastructure.
- The Policy for the Protection of the Cyberspace of the Republic of Poland, adopted by the government in June 2013, sought to "achieve an acceptable level of protection for the state's cyberspace" (Ministry of Administration and Digitization, Internal Security Agency, 2013, p. 6). The key measures proposed in the document were: risk assessment as key to ensuring security, the protection of government administration websites seen as particularly vulnerable infrastructure, legislative action designed to create a legal basis for further policy implementation, the commencement of procedural and organizational efforts aimed at optimizing the performance of Poland's cyberspace, and the launch of educational activities and technical measures aimed at mitigating the above-mentioned risks (Ministry of Administration and Digitization, Internal Security Agency, 2013, pp. 11–17). The document was met with skepticism, its widespread criticism focused primarily on its poor technical quality, the omission of the "good practices" proposed by the European Union Agency for Network and Information Security (ENISA), its inadequate threat analysis, as well as the failure to effectively enforce its provisions (Supreme Audit Office (NIK), 2015, pp. 35–40).
- The Cybersecurity Doctrine of the Republic of Poland, adopted and signed by the President of the Republic of Poland in January 2015, defining a vision for cooperation among individual entities and enumerating key threats (Gapiński, 2016, p. 3). The Doctrine highlights, as its key objective, "ensuring the safe functioning of the Republic of Poland in cyberspace" (National Security Office, 2015, p. 9) by operational means (intended to ensure an acceptable level of security, pursued by public, private and civil sector entities and by trans-sectoral means) and through preparatory action, i.e. by implementing and developing

a systemic approach to cybersecurity in the legal, organizational and technical sense (National Security Office, 2015, pp. 14–22). Although the Doctrine is purely conceptual and the measures it recommends are evidently deficient, it made major progress towards developing a systemic concept, raising the awareness of threats and improving the quality of their analysis.

- The Cybersecurity Doctrine of the Republic of Poland is set to be supplemented by another National Security Office document – the Information Security Doctrine of the Republic of Poland, which is currently in the pipeline. The new addition to the doctrine is meant to address the domestic challenge of the dissemination and reproduction of propaganda content that "portrays Poland's *raison d'état* in a negative light," and the external challenge of the adverse impact of external information and hybrid war (National Security Office, 2015a, pp. 6–8). If and when completed, the document will be combined with its predecessor to form a comprehensive Security Doctrine of the Republic of Poland.

Furthermore, on 23 February 2016, the Ministry of Digitization announced another legislative project in the field of ICT security designed to tackle critical infrastructure, incorporated into the program document: "The Tenets of Cybersecurity Strategy for the Republic of Poland" (Task Force of the Ministry of Digitization, 2016). The document examines the current legal and organizational environment in the field of Poland's cybersecurity and identifies entities endowed with ICT security competencies. Based on the analysis, the main objective has been defined as being to "adopt a legal framework for the national system of cyberspace protection and designate a national body to coordinate the work of other entities in the realm of cyberspace protection" (ibid., p. 6). The priority measures selected in the document are to construct an early warning system, ensure the necessary real-time automatic defense responses, entrust the Ministry of Digitization with the role of system organizer and implement – into the Polish legal system – the Directive of the European Parliament and of the Council concerning measures on a high common level of security of network and information systems across the Union immediately after its entry into force (when the Strategy was prepared, the Directive was still only a draft). Legislative work was also envisioned on a new law on the national cybersecurity system and on amendments to existing laws (ibid., pp. 11–21).

The above assumptions were taken on board in formulating a new Cybersecurity Strategy for 2016–2020, approved by the government in September 2016. To achieve the Strategy's objectives, it was essential to

establish a national cyber security system, coordinate domestic and international activities and lay the groundwork for cooperation with the private sector and academia (Ministry of Digitization, 2016, p. 6). What set the Strategy apart from other documents of its kind was that rather than limiting itself to purely technical considerations, it additionally recognized social considerations having to do with basic human rights and civil liberties. It specifically noted that "cybersecurity is measured not only by the degree of protection against threats to the development of e-commerce, the functioning of the e-state and critical infrastructure, but also by the extent to which unimpeded access to information and its transmission over the Internet, and the ability to use the cyberspace in other ways to exercise fundamental rights has been secured" (ibid., p.7). Specific ideas have also been put forward for trans-sectoral cooperation, as proposed earlier. One of them was to create a Cybersecurity Forum tasked with diagnosing the needs and defining the priorities for such cooperation. While the strategy proposes concrete solutions and sets very ambitious goals, it should also be noted that, similarly to previous documents, it is not legally binding. Thus, the future of cybersecurity in Poland depends on how and to what extent the country achieves the goals set out in the strategy, and especially on whether the legislative measures needed to create the act on the national cybersecurity system are duly taken.

The above shows that while major progress has been made towards ensuring ICT security in Poland, much remains to be done, including, as indicated by a number of authors, the adoption of a single act of primary law, the formulation of a coherent model of action, a clear definition of responsibilities, closer cooperation with the private sector and the spreading of knowledge on cybersecurity (Terlikowski, 2011; Gapiński, 2016, pp. 5–6). Poland has a long way to go to attain an appropriate level of ICT security.

## Conclusions

By and large, the main thesis of the article is that ICT security, defined as "ensuring access to information and its integrity and confidentiality" (Terlikowski, 2011), currently poses one of the biggest challenges faced by the Polish state. The key difficulty lies in the uncertainty as to the exact extent of the problem and the need to develop a multi-faceted approach to tackle it.

To identify fundamental threats, it is vital to examine the problem in a wide range of aspects. The state's key concern are the threats of high-

level attacks on critical infrastructure in the form of cyber espionage and cyberterrorism that could compromise state systems and disrupt institutions. These very threats should be considered a top priority and averted with proper measures.

As all state bodies require a legal basis for the actions they take, it is crucial to draw up and enact laws governing cyberspace. This applies in particular to developing a uniform ICT security strategy and clearly defining the responsibilities of the relevant bodies and institutions responsible for completing the tasks set by the strategy. While a great deal has been done in recent years to formulate legislative proposals for such laws, the majority of the government's proposals are highly general with few guidelines offered on how specifically to pursue the objectives they set. It is therefore crucial to draw up a single legally-binding legislative act that will ultimately resolve the matter. The future ICT security of the Polish state hinges on just such actions.

**Bibliography**

Agencja Bezpieczeństwa Wewnętrznego [Internal Security Agency] (2010), *Bezpieczeństwo teleinformatyczne*, http://bip.abw.gov.pl/bip/informacje-niejawne-1/bezpieczenstwo-teleinf/154,dok.html, 24.11.2016.

Aleksandrowicz T., Bógdał-Brzezińska A., Gryz J., Oleksiewicz I., Ostasz G. (2016), *Terroryzm i cyberterroryzm jako największe wyzwanie bezpieczeństwa współczesnego państwa*, Chicago.

Biuro Bezpieczeństwa Narodowego [National Security Office] (2015), *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf, 29.12.2016.

Biuro Bezpieczeństwa Narodowego (2015a), *Doktryna Bezpieczeństwa Informacyjnego RP. Projekt*, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf, 29.12.2016.

"Financial Times" (2014), *Ukraine PM's office hit by cyber attack linked to Russia*, https://www.ft.com/content/2352681e-1e55-11e4-9513-00144feabdc0, 29.12.2016.

Gapiński K. (2016), *W kierunku systemowego cyberbezpieczeństwa – przegląd dotychczasowych strategii i wnioski dla nowego otwarcia*, "Komentarz Międzynarodowy Pułaskiego", no. 2.

Kozłowski A. (2014), *Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan*, "European Scientific Journal", vol. 3, no. 02, pp. 237–245.

Lakomy M. (2013), *Unia Europejska wobec zagrożeń dla bezpieczeństwa teleinformatycznego – zarys problemu*, "Rocznik Integracji Europejskiej", no. 7, pp. 129–145.

Madej M., Terlikowski M. (2009), *Bezpieczeństwo teleinformatyczne państwa*, Polski Instytut Spraw Międzynarodowych, Warszawa.

Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego [Ministry of Administration and Digitization, Internal Security Agency] (2013), *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, https://mac.gov.pl/files/polityka_ochrony_cyberprzestrzeni_rp_wersja_pl.pdf, 24.11.2016.

McLuhan M. (2011), *The Gutenberg Galaxy*, 16 ed., University of Toronto Press, Toronto.

Ministerstwo Cyfryzacji [Ministry of Digitization] (2016), *Strategia Bezpieczeństwa Rzeczpospolitej Polskiej na lata 2016–2020. Poszanowanie praw i wolności w cyberprzestrzeni. Kompleksowe podejście do bezpieczeństwa. Cyberbezpieczeństwo istotnym elementem polityki państwa*, https://mc.gov.pl/files/strategia_v_29_09_2016.pdf, 29.12.2016.

Ministerstwo Skarbu Państwa [Ministry of Treasury] (2015), *Risk of cyber attacks on Polish SMEs on the rise*, http://www.msp.gov.pl/en/polish-economy/economic-news/6053,Risk-of-cyber-attacks-on-polish-sme-on-the-rise.html, 24.11.2016.

NBC News (2009), *A look at Estonia's cyber attack in 2007*, http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.WDWne4WcHIU, 24.11.2016.

Najwyższa Izba Kontroli [Supreme Audit Office] (2015), *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP*, https://www.nik.gov.pl/plik/id,8764,vp,10895.pdf, 29.12.2016.

Reuters (2015), *Polish airline, hit by cyber attack, says all carriers are at risk*, http://www.reuters.com/article/us-poland-lot-cybercrime-idUSKBN0P21DC20150622, 29.12.2016.

Skrzypczak J. (2011), *Bezpieczeństwo teleinformatyczne w świetle europejskiej Konwencji o cyberprzestępczości*, "Przegląd Strategiczny", issue 1, pp. 51–58.

Terlikowski M. (2011), *Bezpieczeństwo teleinformatyczne wyzwaniem dla Polski*, http://www.geopolityka.org/analizy/712-bezpieczenstwo-teleinformatyczne-wyzwaniem-dla-polski, 22.11.2016.

TVN24 (2016), *Klienci dużego banku na celowniku. Uważaj na takie wiadomości*, http://tvn24bis.pl/z-kraju,74/hakerzy-atakuja-klientow-mbanku,665785.html, 23.11.2016.

TVN24 (2016a), *Problemy w dużym banku, pieniądze "znikały" z kont. "Bardzo przepraszamy"*, http://kontakt24.tvn24.pl/problemy-w-duzym-banku-pieniadze-znikaly-z-kont-bardzo-przepraszamy,217262.html, 23.11.2016.

TVN24 (2016b), *Polacy masowo zastrzegają dokumenty. Sprawdź, dlaczego*, http://tvn24bis.pl/z-kraju,74/polacy-masowo-zastrzegaja-dokumenty,691788.html, 24.11.2016.

Ustawa z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych* [Protection of Classified Information Act], Dz. U. 2010, No. 182, Item 1228, http://isip.sejm.gov.pl/DetailsServlet?id=WDU20101821228, 24.11.2016.

Ustawa z dnia 29 sierpnia 2002 r. *o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*, Dz. U. 2002, No. 156, Item 1301, http://isap.sejm.gov.pl/DetailsServlet?id=WDU20021561301, 24.11.2016.

Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* [Crisis Management Act], Dz. U. 2007, No. 89, Item 590, http://isap.sejm.gov.pl/DetailsServlet?id=WDU20070890590, 24.11.2016.

Zespół zadaniowy Ministerstwa Cyfryzacji [Task Force of the Ministry of Digitization] (2016), *Założenia Strategii Cyberbezpieczeństwa dla Rzeczypospolitej Polskiej*, https://mc.gov.pl/files/zalozenia_strategii_cyberbezpieczenstwa_v_final_z_dnia_22-02-2016.pdf, 29.12.2016.

**Bezpieczeństwo teleinformatyczne jako nowe wyzwanie dla Polski w latach 2007–2017**

## Streszczenie

Celem artykułu jest prezentacja wyzwań stojących przed Rzeczpospolitą Polską w kontekście bezpieczeństwa teleinformatycznego. W analizie dąży się do zdefiniowania znaczenia i zakresu pojęcia bezpieczeństwa teleinformatycznego oraz identyfikacji zagrożeń z jakimi państwo polskie musiało się zmierzyć w ostatniej dekadzie. Nieustanny postęp techniczny powoduje ciągłą ewolucję i szybką dezaktualizację dotychczasowego podejścia. W związku z tym państwo, które chce zapewnić adekwatny poziom ochrony swoim obywatelom stoi przed koniecznością podjęcia odpowiednich środków zaradczych. Mając to na uwadze w dalszej części analizy dąży się do omówienia działań, które w ostatnich latach zostały podjęte przez polskie władze w kierunku realizacji strategicznych celów bezpieczeństwa cyberprzestrzeni państwa. Powyższa analiza pokazuje, że przyszły stan bezpieczeństwa teleinformatycznego państwa polskiego w znacznej mierze zależy od wypracowania jednolitego aktu prawnego.

**Słowa kluczowe:** bezpieczeństwo teleinformatyczne, technologie informacyjne i telekomunikacyjne, regulacje prawne

## About the author

**Martyna Kinga Czyż** [czyz.m.k@gmail.com] has completed an undergraduate program in International Relations (with a specialization in Global Economy and International Business) and graduated from the Faculty of Political Science and Journalism of Adam Mickiewicz University in Poznań. She is currently continuing her education in the same field with a specialization in South-East Asia. Her interests include politics, development economics and post-colonial theory, with a particular focus on Sub-Saharan Africa.