CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Joanna Świątkowska

Izabela Albrycht

Dominik Skokowski

National Cyber Security Organisation: POLAND

Tallinn 2017

www.ccdcoe.org
publications@ccdcoe.org

About NATO CCD COE

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is a NATO-accredited knowledge hub, research institution, and training and exercise facility. The Tallinn-based international military organisation focuses on interdisciplinary applied research, as well as consultations, trainings and exercises in the field of cyber security.

The heart of the Centre is a diverse group of international experts, including legal scholars, policy and strategy specialists who join forces with technology researchers, all from military, government and industry backgrounds.

The Centre is staffed and financed by its sponsoring nations and contributing participants. Belgium, the Czech Republic, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, Turkey, the United Kingdom and the United States are signed on as Sponsoring Nations of NATO CCD COE. Austria, Finland and Sweden have become Contributing Participants, a status eligible for non-NATO nations.

For more information on NATO CCD COE, visit the Centre's website at http://www.ccdcoe.org.

About this study

The NATO CCD COE series of reports on national organisational models for ensuring cyber security summarise national cyber security strategy objectives and outline the division of cyber security tasks and responsibilities between agencies. In particular, the reports give an overview of the mandate, tasks and competences of the relevant organisations and the coordination between them. The scope of the reports encompasses the mandates of political and strategic cyber security governance; national cyber incident management coordination; military cyber defence; and cyber aspects of crisis prevention and crisis management.

Reports in this series

National Cyber Security Organisation in Czech Republic

National Cyber Security Organisation in Estonia

National Cyber Security Organisation in France

National Cyber Security Organisation in Hungary

National Cyber Security Organisation in Italy

National Cyber Security Organisation in Lithuania

National Cyber Security Organisation in the Netherlands

National Cyber Security Organisation in Slovakia

National Cyber Security Organisation in Spain

National Cyber Security Organisation in the United Kingdom

National Cyber Security Organisation in the USA

Non-NATO nations

China: China and Cyber: Attitudes, Strategies, Organisation

National Cyber Security Organisation: Israel

Series editor: Ann Väljataga (Researcher, NATO CCD COE)

Information in this study was checked for accuracy as of December 2016

Contents

1. Digital society in Poland

In Poland in 2016, 80.4% of households had access to the internet and 75.7% had a broadband connection.[1] This is slightly below the European Union (EU) average, but the number is steadily growing.[2] For companies, the figures relating to internet access are significantly higher: 92.5% for small companies (10-45 employees) and 98.8% for medium-sized companies (50-249 employees), or 93.2% of all companies in Poland.[3]

Poles citizens use e-administration less frequently than other Europeans.[4] In 2016, 30.2% of people aged 16-74 used these services, an increase of 3.6% on the figure for 2015. This use was mainly related to obtaining information from public administration websites and submitting applications and reports.[5] In 2015, 93.6% of companies used e-administration services – almost all medium-sized and large companies. Again, the reasons for using e-administration were as primarily related to obtaining information, and downloading and submitting official forms. Some 60.1% of these companies used online services to handle administrative procedures fully electronically.[6]

Currently available e-government services mainly cover taxes and customs services, business activity and public procurements, judicature, labour market, insurance and pensions, public and civil affairs (e.g. registration in the country's electoral roll), healthcare, security and emergency alert, agriculture and rural development, and resources (e.g. disclosure of public data).

The development of e-government is one of the priorities of the Ministry of Digital Affairs of Poland (*Ministerstwo Cyfryzacji*). The Ministry defines efficient e-government platforms as a key factor for the *National Responsible Development Plan,* a strategic plan produced by the Ministry of Economic Development (*Ministerstwo Rozwoju*) to boost economic development of the country to succeed. *The National Computerisation Integrated*

[1] 'Społeczeństwo informacyjne w Polsce w 2016 r.', Główny Urząd Statystyczny, http://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2016-roku,2,6.html.
[2] 'Społeczeństwo informacyjne w Polsce. Wyniki badan statystycznych z lat 2012-2016', Główny Urząd Statystyczny, Urząd Statystyczny w Szczecinie, Warszawa 2016, p. 106.
[3] 'Społeczeństwo informacyjne w Polsce w 2016 r.'.
[4] Śledziewska, Katarzyna, Zięba Damian, 'E-administracja w Polsce na tle Unii Europejskiej. Jak z niej (nie) korzystamy', http://www.delab.uw.edu.pl/wp-content/uploads/2016/10/DELab_e-administracja_w_PL.pdf, 2016, p.5.
[5] 'Społeczeństwo informacyjne w Polsce w 2016 r.'.
[6] Ibid.

Programme[7] is a strategic document describing the government's efforts to provide high-quality electronic public services. The document's annex, titled *State's Computerisation Strategy – the Action Plan of the Minister of Digital Affairs*, presents a set of planned actions related to the computerisation of the key areas of public administration. It includes:[8]

- 'eID – identification in online services' – the creation of a unique point of access to electronic identification services, synchronised with public administration;
- 'Electronic document management' – a unified system of electronic document management in government;
- 'National Registers System' – adoption of a reference model used for data collection, processing and sharing in national registers;
- 'National Major IT Specialist' – base of the national administration know-how, defining the competences of particular entities and the meta-rules of digitalisation processes;
- 'the Republic of Poland Portal' – a portal that will connect government administration's websites in a single, unified and transparent information system.

In terms of e-commerce in Poland, in 2014 there were approximately 13,000 e-shops, 85% of which were micro or small in size. The share of e-commerce in total sales in Poland was approximately 4 to 5%.[9] One year later e-commerce accounted for around 6% of GDP.[10] In 2015 the value of the e-commerce market reached approximately €7.5 billion.[11]

In 2015, online sales in Poland increased by 20%,[12] the number of users having purchased online reached 53%,[13] 34.8% of enterprises sent orders via the internet (31.5% of

[7] 'Program Zintegrowanej Informatyzacji Państwa', Ministerstwo Cyfryzacji, https://mc.gov.pl/konsultacje/program-zintegrowanej-informatyzacji-panstwa/program-zintegrowanej-informatyzacji-panstwa.
[8] 'Strategia Informatyzacji Państwa – Plan Działań Ministra Cyfryzacji', Ministerstwo Cyfryzacji, https://mc.gov.pl/konsultacje/program-zintegrowanej-informatyzacji-panstwa/zalacznik-1-strategia-informatyzacji-panstwa-plan-dzialan-ministra-cyfryzacji.
[9] Kłosiewicz-Górecka, U., 'Zmiany w handlu w okresie chwiejnego rozwoju gospodarczego Polski, Instytut Badań Rynku, Konsumpcji i Koniunktur Polska Organisacja Handlu i Dystrybucji', (presented at the conference 'Handel niezależny i sieciowy w Polsce wobec wyzwań gospodarki opartej na wiedzy', March 2015).
[10] 'Gdzie są granice nasycenia polskiego rynku e-commerce?', https://www.sofort.com/pol-PL/newsroom/prasowe/Gdzie-sa-granice-nasycenia-polskiego-rynku-e-commerce/.
[11] 'Wartość rynku e-commerce to 32-33 mld zł', http://www.dlahandlu.pl/handel-wielkopowierzchniowy/wiadomosci/wartosc-rynku-e-commerce-to-32-33-mld-zl,49646.html.
[12] 'Rynek e-commerce w Polsce – specyfika, trendy, praca', http://www.rp.pl/Biznes/160619670-RYNEK-E-COMMERCE-W-POLSCE--specyfika-trendy-praca.html.
[13] 'E-commerce in Poland: Facts and Figures 2016', quoting: 'We Are Social: 2016 Digital Yearbook', https://www.twenga-solutions.com/en/insights/ecommerce-poland-facts-figures-2016/.

small companies, 44.8% of medium-sized companies), and 12.4% of enterprises received orders via the Internet (10.2% of small companies and 18.8% of medium-sized companies).[14]

2. Strategic national cyber security objectives and cyber security legal framework

2.1. Cyber security policy framework in Poland

There are two main strategic documents purely dedicated to cyber security issues that set up the cyber security landscape by providing the main goals and framing the organisational structure: *Cyberspace Protection Policy of the Republic of Poland*,[15] produced in June 2013 by the former Ministry of Administration and Digitisation (*Ministerstwo Administracji i Cyfryzacji,* MAC) and the Internal Security Agency (Agencja Bezpieczeństwa Wewnętrznego, ABW); and *Cyber Security Doctrine of the Republic of Poland*[16] published in January 2015 by the National Security Bureau (*Biuro Bezpieczeństwa Narodowego*, BBN). Currently, the Ministry of Digital Affairs[17] is preparing a new strategic document, *The Cyber Security Strategy of the Republic of Poland for 2016-2020*, a draft of which is publicly available.[18]

The strategic objective of the Cyberspace Protection Policy is to achieve 'an acceptable level of cyberspace security of the state'.[19] The draft of the new Strategy maintains this goal and provides broader explanation by stating that 'the acceptable level' should be understood as safeguarding capabilities that:[20]

- enable realisation of the state's functions;
- allow to ensure access to essential goods and services for citizens and entrepreneurs;
- ensure undisrupted access to the Internet.

The Policy (and the draft of the Strategy) announces measures that should be undertaken to achieve this objective. It details the creation of a legal and organisational framework and a system for effective coordination and exchange of information between the

[14] 'Społeczeństwo informacyjne w Polsce. Wyniki badan statystycznych z lat 2012-2016'.
[15] 'Cyberspace Protection Policy of the Republic of Poland', Ministry of Administration and Digitisation, Internal Security Agency, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf.
[16] 'Cyber security Doctrine of the Republic of Poland', National Security Bureau, http://en.bbn.gov.pl/en/news/400,Cyber security-Doctrine-of-the-Republic-of-Poland.html.
[17] MAC was disbanded on 16 November 2015 and the Ministry of Digital Affairs replaced it in December 2015.
[18] Even if the final text differs from the draft version, the key directions and decisions are expected to remain.
[19] 'Cyberspace Protection Policy of the Republic of Poland', p. 6.
[20] 'Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020', Ministry of Digital Affairs, p. 4. https://mc.gov.pl/files/strategia_v_29_09_2016.pdf.

entities. These actions are to be built on a risk-based approach. The strategic goal should be met by achieving a set of specific objectives that includes:[21]

1. Increasing the level of security of the state ICT infrastructure.
2. Improving the capacity to prevent and combat threats from cyberspace.
3. Reducing the impact of incidents threatening the ICT security.
4. Determining the competence of entities responsible for the security of cyberspace.
5. Creating and implementing a coherent system of cyberspace security management for all government administration entities and establishing guidelines in this area for non-state actors.
6. Creating a sustainable system of coordination and exchange of information between the entities responsible for the security of cyberspace and the cyberspace users.
7. Increasing awareness of the cyberspace users on the methods and safety measures in cyberspace.

In 2015 the Supreme Audit Office (*Najwyższa Izba Kontroli,* NIK) prepared a special audit to assess implementation of the strategic actions undertaken by the entities responsible for cyber security in Poland.[22] The audit focused heavily on the Policy's provisions. The overall assessment was critical of the success of implementation – the level of the implementation of the key actions and the level of the objectives' achievement were very low.

In parallel with the new Strategy, the Ministry of Digital Affairs is currently working on a bill on cyber security. This should enable it to effectively set up a legal framework for the Polish cyber security system, and clarify the main roles and responsibilities. Hopefully, it will allow for strengthening the capabilities necessary for implementation of the Strategy.

The second strategic document that shapes the cyber security landscape in Poland is the *Cyber Security Doctrine of the Republic of Poland*. The main provisions of the Doctrine are built on the goals included in another document, *The National Security Strategy of the Republic of Poland* (*Strategia Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej,* SBNRP) from 2014. The National Security Strategy states that 'ensuring the security of Poland in cyberspace, including the security of the cyberspace of the Republic of Poland, constitutes one of the basic

[21] 'Cyberspace Protection Policy of the Republic of Poland', pp. 6-7.
[22] 'NIK o bezpieczeństwie w cyberprzestrzeni', https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-w-cyberprzestrzeni.html.

tasks related to the security of the state'.[23] The document points out that the goal should be achieved by developing both defensive and offensive capabilities. A set of actions is laid out, including: cooperation and coordination of protective actions with the private sector, conduct of preventive activities with regard to threats in cyberspace; combating cybercrimes and offenses committed in cyberspace and prosecution of their perpetrators; conduct of the information struggle in the cyberspace, and cooperation with allies.[24]

The Doctrine develops the objectives included in the National Security Strategy, and by introducing operational and preparatory actions, it provides the strategic directions aimed at achieving the main goal – ensuring the cyber security of Poland. The main operational objectives include:

- assessment of the conditions that influence cyber security;
- cyber threat prevention, risk reduction and exploitation of opportunities;
- defence of own ICT system;
- combating sources of threats;
- regaining functionalities of the ICT systems after possible attacks.

In order to achieve operational objectives, preparatory actions must be undertaken which should lead to the development of an intersectoral system consisting of a management subsystem and an operational and supporting subsystem.[25]

The Doctrine is addressed and intends to be a reference material to all the stakeholders whose engagement is needed to achieve the cyber security of Poland: public administration (with the special role of the government), security services, the military, the private sector and citizens.

These documents provide a strategic background for cyber security actions in Poland. They are complemented by a set of documents that regulate various aspects of cyber security presented in ANNEX 1

[23] 'National Security Strategy of the Republic of Poland 2014', National Security Bureau, p. 34. https://www.bbn.gov.pl/ftp/dok/NSS_RP.pdf
[24] Ibid, pp. 34-35.
[25] 'Cyberspace Protection Policy of the Republic of Poland', p. 10.

3. Cyber security Organisational Structure

3.1. Political and strategic management, national cyber policy coordination

Political and strategic responsibility for cyber security and strategic consideration and management is divided between the **Ministry of Digital Affairs** for the civilian dimension and the **Ministry of Defence** (Ministerstwo Obrony Narodowej, MON) for the military (see Chapter 3.3.). Some crucial competences are distributed also between other ministries, agencies and public bodies.

The Ministry of Digital Affairs is a key entity responsible for protecting cyberspace in accordance with the provisions of *the Act on Departments of Government Administration*, and it is obliged, in cooperation with governmental agencies, to achieve the strategic objective of the Policy. The Ministry is particularly responsible for coordinating the implementation of all the actions envisioned by the document, and creating 'regulations which give grounds for further actions in implementing the provisions of the Policy'.[26] The process is supervised by the Council of Ministers.

The Policy states that the Ministry of Digital Affairs should fulfil its obligations with the assistance of a special interdepartmental team appointed by the Prime Minister. The role of the body is mainly to recommend all the actions aimed at implementing the Policy and to recommend future steps.[27] In making strategic decisions, the Ministry is also supported by the **Council for Digitisation** (*Rada do Spraw Cyfryzacji*, RC). The Council gives its opinion on the strategic documents and other documents related to digitisation and cyber security.

The position of the Undersecretary for Cyber Security, whose introduction was announced by the Ministry of Digital Affairs in 2015, has not yet been filled. The Ministry's Department of Cyber Security, created in 2015, performs all tasks related to the coordination of cyber security issues. The main tasks of the Department include: development and implementation of strategic documents and legal acts in the field of cyber security; national and international cooperation (especially with European Union institutions); development of guidelines and standards for the appropriate measures of IT systems protection; preparation of analyses on cyber security and related risks to state security; and development of central training plans, exercises and tests. The Department cooperates with universities, institutes,

[26] Ibid., p. 12.
[27] Ibid., p. 11.

NGOs and the private sector. Since the Ministry supervises the **Research and Academic Computer Network** (Naukowa Akademicka Sieć Komputerowa, NASK), all the tasks related to this function are also carried out by the Department.[28] Key NASK activities are focused on ensuring the security of the internet, and they range from responding to cyber security threats in the network at the operational level (the National Cyber Security Centre (*Narodowe Centrum Cyberbezpieczeństwa,* NCCyber) plays the main role in that matter) to educational and R&D tasks in the field of security, reliability and efficiency of ICT networks.[29]

The National Security Bureau provides guidelines for strategic actions and decisions in the cyber security area. The Doctrine is not a legally binding document, but rather shapes the political and strategic approach to cyber security in Poland. So, it can be only a point of reference for these governmental entities in establishing a national cyber security system. There is no legislative basis for the National Security Bureau to be formally involved in the process of national cyber security policy coordination, but it can be consulted and can invite representatives of governmental institutions and agencies to participate in the process of drawing up guidelines. The Bureau's Department of Law and Non-Military Security is responsible for cyber security issues. There is also a special Team for Cyberspace Security that consists of representatives of the National Security Bureau and external experts and is responsible for updating the Doctrine.

Other public bodies with major responsibilities regarding cyber security management are:

- The **Ministry of Justice** (*Ministerstwo Sprawiedliwości,* MS) creates the law on cybercrime and oversees its proper execution.
- The **Ministry of the Interior and Administration** (*Ministerstwo Spraw Wewnętrznych i Administracji*, MSWiA) monitors the actions of the police in combating cybercrime and is responsible for crisis management. It oversees the National Police Headquarters responsible for combating cybercrime (the Department of Support in Fighting Cybercrimes operates within the structures of the Bureau of Criminal Investigation).[30]

[28] Department of Cyber security**,** Ministry of Digital Affairs, https://mc.gov.pl/en/department-of-cyber-security**.**
[29] 'About NASK', Research and Academic Computer Network, http://eng.nask.pl/en/about-nask/about-nask/250,Research-and-Academic-Computer-Network.html.
[30] 'Zwalczaj cyberprzestępczość', http://www.policja.pl/pol/zwalczaj-cyberprzestep/83643,Zwalczaj-cyberprzestepczosc.html.

- The Internal Security Agency (Agencja Bezpieczeństwa Wewnętrznego, **ABW)** is a governmental institution which protects the internal security of Poland and its citizens, including the execution of tasks within the scope of IT systems security dedicated to processing confidential data (more on the Agency's tasks and responsibilities in Section 3.5).
- The **Government Centre for Security** (Rządowe Centrum Bezpieczeństwa, RCB) is an institution accountable to the Prime Minister that is involved in crisis management at the governmental level. It plays the main role in the creation of the critical infrastructure (CI) security system in Poland including the cyber security dimension. The director of the Centre, together with ministers and managers of particular Central Offices, prepares domestic and European Critical Infrastructure (CI) lists and maintains the National Critical Infrastructure Security Programme.[31]
- **Office of Electronic Communications** (*Urząd Komunikacji Elektronicznej*, UKE) is a regulator of the telecommunications market supervised by the Ministry of Digital Affairs that provides the implementation of the Telecommunications Act in the context of cyberspace security and acquires information about security incidents and the integrity of telecommunications networks from network providers and telecommunications services and sends them, inter alia, to ENISA.[32]
- The Polish **Financial Supervision Authority** (*Komisja Nadzoru Finansowego*, KNF) is a financial regulatory authority that provides recommendations on the Management of Information Technology and ICT Environment Security at Banks.[33]
- The **Inspector General for the Protection of Personal Data** (*Generalny Inspektor Ochrony Danych Osobowych*, GIODO) is a public body empowered to supervise compliance of data processing with the provisions on the protection of personal data, issue administrative decisions and consider complaints with respect to the enforcement of the provisions on the protection of personal data, issue opinions on

[31] Świątkowska, J. (edit.), 'Critical Infrastructure Security – the ICT Dimension', The Kosciuszko Institute, 2014, p.128.
[32] 'Informowanie o naruszeniach bezpieczeństwa lub integralności sieci', https://www.uke.gov.pl/informowanie-o-naruszeniach-bezpieczenstwa-lub-integralnosci-sieci-16943.
[33] 'Recommendation D On the Management of Information Technology and ICT Environment Security at Banks', Polish Financial Supervision Authority, https://www.knf.gov.pl/Images/RecommendationD_tcm75-44254.pdf.

bills and regulations with respect to the protection of personal data, and to initiate and undertake activities aimed at improving the protection of personal data.[34]

The current distribution of competences among governmental cyber security stakeholders in Poland is often contested. Therefore, we can expect shifts of responsibility in the future. One of the recommended models is a structure under the Prime Minister's Office.

3.2. Operational cyber security capabilities, cyber incident management and coordination

The current model of cyber security strategic and institutional coordination presented in Section 3.1 often comes under criticism, whereas the operational and cyber incident management system is praised for its effectiveness and its fast responses to attacks directed against ICT systems and offered services.

The Policy established a three-level National Response System for Computer Security Incidents in cyberspace with the following assignation:

1) Level I – the level of coordination – the minister responsible for informatisation (Ministry of Digital Affairs);

2) Level II – computer incident response:

a) the **Governmental Computer Security Incident Response Team** – CERT.GOV.PL – performs the role of the main CERT in the area of emergency responses within the government administration and the civil area and coordinates the process of handling computer incidents in cyberspace. The team was established in 2008 and has been operating within the structures of the Internal Security Agency.[35] 'CERT.GOV.PL engages with and considers as its prime 'constituency' all the users of ICT systems within the public administration (.gov.pl domain) and entities that comprise the critical ICT infrastructure of the state;'[36]

b) **MIL-CERT PL** (also known as Polish Military Computer Incident Response Team – System Reagowania na Incydenty Komputerowe, SRnIK – covered in Section 3.3);

3) Level III – the level of implementation – administrators responsible for individual ICT systems.

[34] 'Responsibilities of the inspector general for personal data protection', http://www.giodo.gov.pl/138/id_art/368/j/en/.
[35] 'About us', CERT.GOV.PL Team, http://www.cert.gov.pl/cee/main-site-about-us/77,About-us.html.
[36] Maj, M., 'Critical infrastructure and incident response', in: 'Critical Infrastructure Security – the ICT Dimension', Świątkowska, J. (edit.), The Kosciuszko Institute, 2014, p. 84.

Within the structure of NASK as part of the National Cyberspace Protection System, the **NCCyber** was created in 2016. The legal basis of NCCyber is going to be introduced in the new bill on cyber security. It operates in the private-public cooperation model. It is active in the field of research, operational tasks, training and analytics. As an early warning centre, it is responsible for the security of Polish cyberspace and for quick reactions to any incidents targeting cyber security. This operational part of NCCyber is a new National CERT. CERT Polska is authorised to address and coordinate all types of computer security incidents which occur, or threaten to occur across .pl domain hosts and to implement incident response measures. CERT Polska exchanges all necessary information with other CSIRTs and with affected parties' administrators.[37]

NCCyber is also tasked with developing the national protection plans. It cooperates with administration, commercial enterprises and with the research environment and its Operational Centre is continually manned and monitors network-related threats and manages the exchange of related information.[38]

Other Computer Security Incident Response Teams:

- The PIONIER-CERT (former: POL34-CERT) has been established to provide effective incident response service to members and users of Polish Scientific Broadband Network PIONIER;.[39]
- CERT ORANGE POLSKA (previously TP CERT) ensures the safety of users of the Orange Polska SA telecommunications network.[40]

Poland participates in TF-CSIRT and FIRST, and cooperates in international cyber security activities with ENISA and NATO.

The presented structure is likely to change due to the process of updating the Strategy and introducing new bill on cyber security and a notion of creating sectoral CSIRTs.

[37] 'CSIRT Description for CERT Polska', https://www.cert.pl/wp-content/uploads/2015/11/rfc2350.txt.
[38] 'Opening of NCCyber', http://eng.nask.pl/en/news/events/events-2016/262,Opening-of-NC-Cyber.html.
[39] 'About us', PIONIER-CERT, https://cert.pionier.gov.pl/HomePage.
[40] 'Czym jest CERT', CERT Orange Polska, https://www.cert.orange.pl/.

3.3. Military cyber defence

a) Policies and laws

Polish priorities and challenges in regard to military cyber defence are broadly defined in *The National Security Strategy of the Republic of Poland.*[41] It stipulates the need for development of both defensive and offensive cyber capabilities along with new units within the Armed Forces dedicated to this goal. The National Security Strategy also stresses the need to enhance preparedness for any incidence of cyber war and the country's ability to react, either unilaterally or with the cooperation of allies.

The Doctrine further elaborates on military cyber defence.[42] Amongst other things, it stipulates the need for the implementation of NATO standards in regard to operational and defence planning. Emphasis is also put on the development of domestic solutions and access to source codes of foreign software used in systems of importance to national security. As in the National Security Strategy, there is an imperative to develop defensive and offensive cyber capabilities.

From a practical standpoint, the response to a severe cyber-attack can be coordinated via the declaring of either a state of emergency,[43] a state of natural disaster[44] or martial law.[45] Respective bills regulating each of those consider a cyberspace incident as a triggering force. Serious cyber-attacks can be managed by means described in the Crisis Management Act (covered in Section 3.4.).[46]

Under threat or instance of any kind of terrorist event which affects the ICT system of public administration or critical infrastructure, the counterterrorism legislation[47] allows the

[41] 'National Security Strategy of the Republic of Poland 2014'.
[42] 'Cyber Security Doctrine of the Republic of Poland'.
[43] 'Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym', Sejm RP, http://isap.sejm.gov.pl/DetailsServlet?id=WDU20070890590.
[44] 'Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej', Sejm RP, http://isap.sejm.gov.pl/DetailsServlet?id=WDU20020620558.
[45] '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', Sejm RP.
[46] 'Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym', Sejm RP, http://isap.sejm.gov.pl/DetailsServlet?id=WDU20070890590.
[47] 'Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych', Sejm RP, http://isap.sejm.gov.pl/DetailsServlet?id=WDU20160000904.

implementation of a scale of four security alarms. Particular coordinating procedures for ensuring security are regulated by a specific regulation from the Prime Minister.[48]

b) Organisational structure and key entities

The highest ranking official in the Polish government responsible for military cyber defence is the **Minister of Defence**. Their responsibilities are described in the draft version of the Strategy[49] as:

- overseeing national defence;
- ensuring armed forces acquire and retain full operational capability in terms of defensive and offensive cyber potential;
- organising operations in times of threat of war or during wartime with use of defensive planning mechanisms;
- taking charge of cyber security systems during higher states of readiness;
- setting the operating rules of National CSIRT during crisis or wartime; and
- cooperation with other cyber security system stakeholders.

Since 2012, within the Ministry of Defence a function of Plenipotentiary of the Minister of Defence Responsible for the Security of Cyberspace has been appointed.[50] Among their responsibilities are the coordination of tasks belonging to the Minister of Defence, supporting other units within the Ministry in ensuring its cyber security, supervising the implementation of laws and policies, cooperation with the **Military Counterintelligence Service** (Służba Kontrwywiadu Wojskowego, SKW), providing information about the current state and risks related to cyberspace, and representing the Ministry in joint working groups within NATO and EU.

The **National Cryptology Centre** (Narodowe Centrum Kryptologii, NCK) established in 2013 within the Ministry of Defence has been tasked with coordinating the ministry's activities

[48] 'Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP', Dziennik Ustaw RP, http://www.dziennikustaw.gov.pl/du/2016/1101/1.
[49] 'Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020', p. 10.
[50] 'Decyzja Nr 38/MON z dnia 16 lutego 2012 r. w sprawie powołania Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni', http://www.dz.urz.mon.gov.pl/dziennik/pozycja/decyzja-52-decyzja-nr-38mon-z-dnia-16-lutego-2012-r-w-sprawie-powolania-pelnomocnika-ministra-obrony-narodowej-do-spraw-bezpieczenstwa-cyberprzestrzen/.

within the area of cyber protection, even though statutory responsibilities of the unit relate only to cryptology. The NCK's Director is currently the Head of the SKW.

On the defensive side, within the Ministry of Defence the unit responsible for securing the Polish military network is **MIL-CERT PL** established in 2008.[51] MIL-CERT's mission is 'to provide the capability to deal with computer security incidents in Polish military networks and assist constituency in implementing proactive measures to reduce the risks of computer security incidents'.[52] It is organised in three tiers.[53] The first tier consists of a Coordination Centre (Centrum Koordynacyjne, CK) run by a sub-unit within the Military Counterintelligence Service. The second consists of a Technical Support Centre (Centrum Wsparcia Technicznego, CWT) which has the responsibilities and duties of a CERT. The third consists of system administrators of various units within the Ministry. MIL-CERT PL is under the joint supervision of the Plenipotentiary of the Minister of Defence for the Security of Cyberspace and the Head of the Military Counterintelligence Service.

The Cyber Security Centre (Centrum Bezpieczeństwa Cybernetycznego, CBC) was created within the Ministry of Defence in 2010 to develop military cyber capabilities. The unit operates under the National Cryptology Centre. The Cyber Security Centre was disbanded in 2015 and the **Cybernetic Operations Centre** (Centrum Operacji Cybernetycznych, COC) was created in its place. Specific activities of this unit are classified.

The unit responsible for digitisation within the Ministry of Defence is the **Information Systems Inspectorate** (Inspektorat Systemów Informatycznych, ISI). Among its responsibilities is ensuring security of the systems belonging to the Minister of Defence.[54]

c) R&D and financing

Poland's Armed Forces Technical Modernisation Programme for 2017-2022 has, for the first time, a component dedicated solely to the development of cyber capabilities as a priority programme. The draft project included formation of a new lab and several

[51] 'Decyzja Nr 275/MON z dnia 13 lipca 2015 r. w sprawie organisacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej', Dziennik Urzędowy MON, http://www.dz.urz.mon.gov.pl/dziennik/pozycja/decyzja-208-decyzja-nr-275mon-z-dnia-13-lipca-2015-r-w-sprawie-organisacji-i-funkcjonowania-systemu-reagowania-na-incydenty-komputerowe-w-resorcie-obr/.
[52] 'CSIRT Description for SRnIK', http://srnik.wp.mil.pl/plik/file/srnik/rfc2350.txt.
[53] 'O SRnIK', Ministerstwo Obrony narodowej, http://srnik.wp.mil.pl/pl/index.html.
[54] 'ISI – Zadania', Inspektorat Systemów Informacyjnych, http://isi.wp.mil.pl/pl/3.html.

programmes designed to develop software and hardware to enhance the cyber capabilities of the armed forces.[55]

The **National Centre for Research and Development** (Narodowe Centrum Badań i Rozwoju, NCBiR), the institution responsible for allocating public funds in R&D projects, is cooperating with the Minister of the Interior and the Minister of Defence in organising grants to encourage the development of defence technologies, including information technologies.[56]

3.4. Crisis prevention and crisis management

Cyber threats are in the recognised catalogue of threats which may lead to a crisis situation in Poland. Crisis management in Poland is divided into four phases: prevention, preparation, reaction, and reconstruction. Under the *Act of 26 April 2007 on Crisis Management*[57] and in the updated *National Crisis Management Plan 2013/2015*,[58] the Head of the Internal Security Agency is responsible for crisis management and the protection of critical infrastructure and counteracting threats in cyberspace. Crisis management requires the involvement and cooperation of multiple central and local government entities, and it is assisted by a number of supporting institutions.

In the prevention phase, the Head of the Internal Security Agency, through CERT.GOV.PL and the IT Security Department, implements tasks including protection of classified information, the accreditation of systems for classified information processing, and the examination and assessment of security as part of the certification process. Its tasks also include increasing the awareness and knowledge of public administration employees regarding cyber threats, developing the ability of organisational units of governmental administration to protect themselves against cyber threats, implementing tasks in the scope of Level II responses, creating catalogues of threats and potential vulnerabilities, and preparing guidelines and instructions for government administration. The Agency also plays the role of a National Focal Point as part of NATO Policy on Cyber Defence. It liaises with the following supporting institutions:

[55] Zieliński, K., presentation at 24th International Defence Industry Exhibition MSPO in Kielce, 6-9 September, 2016.
[56] Bondaryk, K., 'MON bezbronne w cyberprzestrzeni', http://www.altair.com.pl/news/view?news_id=18223.
[57] 'Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym'.
[58] National Crisis Management Plan 2013/2015, Rządowe Centrum Bezpieczeństwa, http://rcb.gov.pl/wp-content/uploads/KPZK-2013-2015.tj_..pdf, pp. 334-361.

- Ministry of the Interior and Administration;
- Ministry of Digital Affairs;
- Ministry of Defence;
- Ministry of Treasury (Ministerstwo Skarbu Państwa, MSP);
- Ministry of Science and Higher Education (Ministerstwo Nauki i Szkolnictwa Wyższego – MNiSW*)*;
- Ministry of National Education (Ministerstwo Edukacji Narodowej – MEN);
- Foreign Intelligence Agency (Agencja Wywiadu, AW);
- The Government Centre for Security (Rządowe Centrum Bezpieczeństwa, RCB);
- Council of Ministers;
- President of the Council of Ministers; and
- Regional officials.

In the preparation phase, the following bodies are involved in a supporting capacity:

- Ministry of the Interior and Administration;
- Ministry of Digital Affairs;
- Ministry of Defence;
- Ministry of Treasury;
- The Government Centre for Security;
- Council of Ministers; and
- Regional officials.

For the Agency, this phase involves, issuing recommendations in the scope of ICT security, training in the scope of ICT security for the administrators of IT systems in governmental administration, conducting safety tests, developing a system for early warning against cyberthreats, and the implementation and maintenance of preventive solutions.[59]

In the reaction phase, the Head of the Internal Security Agency is responsible for the coordination of the process of handling computer incidents in government administration, cyberthreat detection, recognition and counteraction, providing information to the administrators when errors are detected in IT systems, handling incidents in networks covered by the protection of the ARAKIS-GOV system, publication of alerts and warnings, conducting post-breach analyses, and preparation of recommendations aimed at increasing the safety of

[59] Ibid, p. 347.

government ICT systems.[60] The supporting institutions in that phase are: the Ministry of the Interior and Administration, Ministry of Digital Affairs, Ministry of Treasury, Ministry of Defence, the Government Centre for Security, President of the Republic of Poland, Council of Ministers and the Voivode.

In the reconstruction phase, as part of which CERT.GOV.PL is responsible for conducting post-breach analyses, the supporting institutions are: the Ministry of the Interior and Administration, Ministry of Treasury, Ministry of Defence, Foreign Intelligence Agency, The Government Centre for Security and Regional officials.

The list of activities allocated to each entity is detailed and only a few have been mentioned in this Chapter.

3.5. Cyber intelligence

There are four major Polish intelligence agencies, each of which have different priorities and capabilities in terms of cyber security. Those are two non-military agencies: the Foreign Intelligence Agency (Agencja Wywiadu, AW) and Internal Security Agency (Agencja Bezpieczeństwa Wewnętrznego, ABW); and two military agencies: the Military Intelligence Service (Służba Wywiadu Wojskowego, SWW) and Military Counterintelligence Service (Służba Kontrwywiadu Wojskowego, SKW).

a) Foreign Intelligence Agency (AW)

The AW addresses external threats to the security of the country. Among its tasks strictly related to cyber security is ensuring the protection of cryptographic communication with Polish diplomatic missions and conducting signals intelligence.[61]

b) Internal Security Agency (ABW)

The ABW is responsible for counterintelligence and counterterrorism within Poland,[62] and has a dedicated IT Security Department and specialised regional divisions.[63] The Agency is also responsible for counterterrorism, including in the cyber dimension. Within the structure of the Agency is the Governmental Computer Security Incident Response Team CERT.GOV.PL

[60] Ibid, p. 352.
[61] 'Status of the Foreign Intelligence Agency', Agencja Wywiadu, http://www.aw.gov.pl/eng/agencja/przedmiot-dzialania-agencji.html.
[62] 'System bezpieczeństwa cyberprzestrzeni RP', NASK, 2015, p. 5.
[63] 'Bezpieczeństwo teleinformatyczne', Agencja Bezpieczeństwa Wewnętrznego, http://www.bip.abw.gov.pl/bip/informacje-niejawne-1/bezpieczenstwo-teleinf/154,dok.html.

which acts as the primary CERT in the area of government administration and the civil area. 'Its chief task is ensuring and developing the capability of public administration units to protect themselves against cyberthreats, in particular against attacks aimed at the infrastructure involving IT systems and networks'.[64] The Counterterrorism Act of June 2016 empowers the Head of the Internal Security Agency with a broad array of tools to prevent and counteract terrorism, such as accessing and recording conversations and correspondence conducted via telecommunication networks and accessing and collect information on data, end-user tools and ICT systems. the Head of the Internal Security Agency can order access to the information about the structure and functioning of an ICT system such as a computer password, access codes and other data which allows access to the system. The set of tools at his disposal contains also the denial of access, in other words, possibility for a court to order a blockage of access to particular data included in the ICT system, which is connected to terrorist activity.[65]

c) Military Intelligence Service (SWW)

The Military Intelligence Service is a special service, whose fields of interests concern international threats to state defence security, the safety and operational ability of the Armed Forces and other administrative units supervised by the Minister of National Defence. Its main goal is to identify and counteract external military threats and terrorism. The SWW takes part in an exchange of information and practices with respective agencies of NATO allies and EU member states, including matters related to cyber security.[66]

d) Military Counterintelligence Service (SKW)

The SKW is responsible for the protection of the country against internal threats to national defence, security and combat effectiveness of the armed forces and other organisational units supervised by the Minister of National Defence. It is a public administration office governed by the Minister of National Defence.[67] The main tasks of the SKW within the cyber security domain are protection of classified information, cryptography (the Service issues certificates of cryptographic tools), cryptanalysis and electronic

[64] Świątkowska, J., 'Cyber Security in Poland', in: 'V4 Cooperation in Ensuring Cyber Security – Analysis and Recommendations', Świątkowska J. (edit.), The Kosciuszko Institute, 2012, p. 45.
[65] Świątkowska, J., Szwiec, M., Llacayo, A., 'Make a Bomb in the Kitchen of Your Mom – How Terrorists Use Cyberspace and How to Fight with Them', The Kosciuszko Institute Policy Brief, 2016.
[66] 'System bezpieczeństwa cyberprzestrzeni RP', NASK, September 2015, p. 17. https://www.cert.pl/wp-content/uploads/2015/12/nask_rekomendacja.pdf.
[67] 'About MCS', Służba Kontrwywiadu Wojskowego, http://www.skw.gov.pl/en/o-skw.html.

counterintelligence.[68] Since April 2016 there has been an Office of Cyber Security (Biuro Bezpieczeństwa Cybernetycznego, BBC) within the SKW. The head of the Military Counterintelligence Service is also Head of the National Cryptology Centre. The Service supervises the work of MIL-CERT PL as part of its activities related to classified networks.

The SKW (along with the AWB) is also responsible for certifying electronic communication tools and appliances with the ability to protect classified information.

3.6. Private sector involvement and cooperation with industry

The Telecommunications Act (as updated in 2012) requires telecommunications companies to report cyber incidents to the national telecommunications regulator, the UKE. The law was accompanied by a decision from the Minister of Administration and Digitisation in 2013[69] which details the severity thresholds for reporting. However, as was found by the Supreme Audit Office in 2015[70] that ambiguities in the regulations make it impossible for the Chairman of the UKE to effectively gather and process information about incidents from telecommunication companies.

Critical infrastructure operators in Poland are responsible for ensuring the security and integrity of their infrastructure as required by the 2007 Crisis Management Law.[71] However, most of the cooperation with public entities is voluntary.

The private sector in Poland is engaged in various government-led initiatives related to cyber security. NCCyber, which operates within the structure of NASK, is one of them.[72] Launched on July 4, 2016 NCCyber signed partnership agreements with leading companies operating in Poland: telecoms (Orange, Polkomtel, TMobile), energy (Energa, PSE, Gaz System, PERN), banking (Bank Handlowy w Warszawie, BZ WBK, Credit Agricole, mbank, PKO BP) and transportation (PKP Informatyka). More have since followed, although the full list is classified.

---

[68] 'Zadania SKW', Służba Kontrwywiadu Wojskowego, http://www.skw.gov.pl/en/zadania.html.
[69] 'Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 19 marca 2013 r. w sprawie wzoru formularza do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług', Sejm RP, http://isap.sejm.gov.pl/DetailsServlet?id=WDU20130000386.
[70] 'Realisacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP', NIK, p. 45. https://www.nik.gov.pl/plik/id,8764,vp,10895.pdf.
[71] 'Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym'.
[72] 'NC Cyber – Narodowe Centrum Cyberbezpieczeństwa', NASK, https://www.nask.pl/pl/dzialalnosc/nc-cyber/142,NC-Cyber-Narodowe-Centrum-Cyberbezpieczenstwa.html

In 2016, the national oil transportation company PERN signed a bilateral agreement with NASK to comprehensively enhance its level of cyber security.[73] The agreement was the first of its kind and can be described as an example of best practice. Under the agreement, NASK provides comprehensive services spanning consultation, hardware, software, know-how and experts to secure the company's infrastructure.

Also in 2016, the national electricity transmission company PSE signed an agreement with the NATO Energy Security Centre of Excellence outlining cooperation within the domain of critical infrastructure protection.[74] Cyber security was one of the central points of the agreement. PSE was the first Polish body to establish this kind of cooperation with the Centre.

There are also bottom-up initiatives that contribute to the national cyber capabilities. One worth noting is **Polish Citizens' Cyber Defence** (Polska Obywatelska Cyberobrona), launched in 2015.[75] The association's goal is to gather cyber security specialists willing to voluntarily contribute to national security in case of emergency.

[73] 'PERN - cyberbezpieczny!', PERN, http://pern.pl/pern-cyberbezpieczny/.
[74] 'Umowa PSE-NATO ws. ochrony infrastruktury elektroenergetycznej', http://www.pap.pl/aktualnosci/news,536936,umowa-pse-nato-ws-ochrony-infrastruktury-elektroenergetycznej.html.
[75] 'Powstaje Polska Obywatelska Cyberarmia'. https://www.cybsecurity.org/powstaje-polska-obywatelska-cyberobrona/.

ANNEX 1.

Selection of the most important acts that include cyber security elements added to the documents described in the chapter 1.

TITLE OF THE LAW	THE MAIN SCOPE OF THE REGULATION
Act on Government Administration of 4 September 1997	the Governments' scope of responsibilities
Act on Martial Law and the competence of the Commander-in-Chief and his subordination to the constitutional authorities of the Republic of Poland of 29 August 2002	provides a law framework for extraordinary actions undertaken in case of introduction of martial law caused by cyberattacks
Act on the State of Emergency of 21 June 2002	provides a law framework for extraordinary actions undertaken in case of emergency state caused by cyberattacks
Act on the State of Natural Disaster of 18 April 2002	provides a law framework for extraordinary actions undertaken in case of state of natural disaster caused by cyberattacks
Act on Crisis Management of 26 April 2007	provides a key framework for crisis management and critical infrastructure protection
Act on the Protection of Classified Information of 5 August 2010	protection of classified information
Act on the Protection of Personal Data of 29 August 1997	personal data protection
Act on Anti-Terrorist Activities of 10 June 2016	rights and obligations of entities that combat terrorist acts (including actions relevant from the cyber security point of view).
Act on the Internal Security Agency and the Intelligence Agency of 24 May 2002	responsibilities of two agencies: ISA, responsible for internal security and counterespionage activities, and IA, responsible for intelligence activities
Act on Police of 6 June 1990	responsibilities of the main entities that combat cybercrime
Banking Act of 29 August 1997	actions undertaken to safeguard the banking sector
Telecommunications Act of 16 July 2004	introduces obligations related to cyber security for telecommunications operators
Act on the Informatisation of Entities Performing Public Tasks of 17 February 2005	provides a basis for security requirements of the IT systems used by the entities performing public tasks
Act on Providing Services by Electronic Means of 18 July 2002	provides a basis for security requirements of the services provided by the security means
Act on Trust Services and Electronic Identification of 5 September 2016	provides a basis for security requirements of the trust services and electronic identification

References

POLICY

Ministry of Administration and Digitisation, Internal Security Agency. 2013. 'Cyberspace Protection Policy of the Republic of Poland'. Accessed September 9, 2016. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf.

Ministry of Digital Affairs. 2016. 'Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020'. Accessed September 9, 2016. https://mc.gov.pl/files/strategia_v_29_09_2016.pdf.

National Security Bureau. 2014. 'National Security Strategy of the Republic of Poland'. Accessed September 9, 2016. https://www.bbn.gov.pl/ftp/dok/NSS_RP.pdf.

National Security Bureau. 2015. 'Cyber security Doctrine of the Republic of Poland'. Accessed September 9, 2016. http://en.bbn.gov.pl/en/news/400,Cyber security-Doctrine-of-the-Republic-of-Poland.html.

Rządowe Centrum Bezpieczeństwa, 'National Crisis Management Plan 2013/2015'. Accessed Decemebr 18, 2016. http://rcb.gov.pl/wp-content/uploads/KPZK-2013-2015.tj_..pdf.

LAW

Dziennik Ustaw RP, 'Rozporządzenie Prezesa rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP'. Accessed November 7, 2016. http://www.dziennikustaw.gov.pl/du/2016/1101/1.

Dziennik Urzędowy MON, 'Decyzja Nr 275/MON z dnia 13 lipca 2015 r. w sprawie organisacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej'. Accessed November 7, 2016. http://www.dz.urz.mon.gov.pl/dziennik/pozycja/decyzja-208-decyzja-nr-275mon-z-dnia-13-lipca-2015-r-w-sprawie-organisacji-i-funkcjonowania-systemu-reagowania-na-incydenty-komputerowe-w-resorcie-obr/.

Dziennik Urzędowy MON, 'Decyzja Nr 38/MON z dnia 16 lutego 2012 r. w sprawie powołania Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni'. Accessed November 7, 2016. http://www.dz.urz.mon.gov.pl/dziennik/pozycja/decyzja-52-decyzja-nr-38mon-z-dnia-16-lutego-2012-r-w-sprawie-powolania-pelnomocnika-ministra-obrony-narodowej-do-spraw-bezpieczenstwa-cyberprzestrzen/.

Sejm RP, 'Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 19 marca 2013 r. w sprawie wzoru formularza do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług'. Accessed November 7, 2016. http://isap.sejm.gov.pl/DetailsServlet?id=WDU20130000386.

Sejm RP, 'Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej'. Accessed November 7, 2016. http://isap.sejm.gov.pl/DetailsServlet?id=WDU20020620558

Sejm RP, ‘Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym’. Accessed November 7, 2016. http://isap.sejm.gov.pl/DetailsServlet?id=WDU20070890590.

Sejm RP, ‘Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym’. Accessed November 7, 2016. http://isap.sejm.gov.pl/DetailsServlet?id=WDU20070890590.

Sejm RP, ‘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’. Accessed November 7, 2016. http://isap.sejm.gov.pl/DetailsServlet?id=WDU20021561301.

Sejm RP, ‘Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych’. Accessed November 7, 2016. http://isap.sejm.gov.pl/DetailsServlet?id=WDU20160000904.

OTHERS

Agencja Bezpieczeństwa Wewnętrznego, ‘Bezpieczeństwo teleinformatyczne’. Accessed December 18, 2016. http://www.bip.abw.gov.pl/bip/informacje-niejawne-1/bezpieczenstwo-teleinf/154,dok.html.

Agencja Wywiadu, ‘Status of the Foreign Intelligence Agency’. Accessed November 7, 2016. http://www.aw.gov.pl/eng/agencja/przedmiot-dzialania-agencji.html

Bondaryk, Krzysztof, ‘MON bezbronne w cyberprzestrzeni’. Accessed November 7, 2016. http://www.altair.com.pl/news/view?news_id=18223.

CERT Orange Polska, ‘Czym jest CERT’. Accessed December 19, 2016, https://www.cert.orange.pl/.

CERT.GOV.PL Team, ‘About us’. Accessed December 19, 2016. http://www.cert.gov.pl/cee/main-site-about-us/77,About-us.html.

CSIRT Description for CERT Polska. Accessed December 19, 2016. https://www.cert.pl/wp-content/uploads/2015/11/rfc2350.txt.

CSIRT Description for SRnIK. Accessed November 7, 2016. http://srnik.wp.mil.pl/plik/file/srnik/rfc2350.txt

E-commerce in Poland: Facts and Figures 2016, quoting: ‘We Are Social : 2016 Digital Yearbook‘. Accessed October 10, 2016. https://www.twenga-solutions.com/en/insights/ecommerce-poland-facts-figures-2016/.

Gdzie są granice nasycenia polskiego rynku e-commerce?. Accessed October 13, 2016. https://www.sofort.com/pol-PL/newsroom/prasowe/Gdzie-sa-granice-nasycenia-polskiego-rynku-e-commerce/.

Główny Urząd Statystyczny, ‘Społeczeństwo informacyjne w Polsce w 2016 r.’. Accessed November 11, 2016. http://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2016-roku,2,6.html.

Informowanie o naruszeniach bezpieczeństwa lub integralności sieci. Accessed December 18, 2016. https://www.uke.gov.pl/informowanie-o-naruszeniach-bezpieczenstwa-lub-integralnosci-sieci-16943.

Inspektorat Systemów Informacyjnych, 'ISI – Zadania' Accessed November 7, 2016. http://isi.wp.mil.pl/pl/3.html.

Kłosiewicz-Górecka, Urszula, 'Zmiany w handlu w okresie chwiejnego rozwoju gospodarczego Polski, Instytut Badań Rynku, Konsumpcji i Koniunktur Polska Organisacja Handlu i Dystrybucji', March 2015 (presented at the conference 'Handel niezależny i sieciowy w Polsce wobec wyzwań gospodarki opartej na wiedzy').

Maj, Mirosław, 'Critical infrastructure and incident response', in: 'Critical Infrastructure Security – the ICT Dimension', Świątkowska, Joanna. (edit.), The Kosciuszko Institute, 2014.

Ministerstwo Obrony Narodowej, 'O SRnIK' Accessed November 7, 2016. http://srnik.wp.mil.pl/pl/index.html.

Ministry of Digital Affairs, Department of Cyber security, Accessed December 18, 2016. https://mc.gov.pl/en/department-of-cyber-security.

NASK, 'NC Cyber – Narodowe Centrum Cyberbezpieczeństwa'. Accessed November 7, 2016. https://www.nask.pl/pl/dzialalnosc/nc-cyber/142,NC-Cyber-Narodowe-Centrum-Cyberbezpieczenstwa.html.

NASK, 'System bezpieczeństwa cyberprzestrzeni RP'. Accessed December 10, 2016. https://www.cert.pl/wp-content/uploads/2015/12/nask_rekomendacja.pdf.

NIK o bezpieczeństwie w cyberprzestrzeni. Accessed June 30, 2016. https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-w-cyberprzestrzeni.html.

NIK, 'Realisacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP', p. 45. Accessed November 7, 2016. https://www.nik.gov.pl/plik/id,8764,vp,10895.pdf.

Opening of NC Cyber. Accessed December 19, 2016, http://eng.nask.pl/en/news/events/events-2016/262,Opening-of-NC-Cyber.html.

PERN, 'PERN - cyberbezpieczny!'. Accessed November 7, 2016. http://pern.pl/pern-cyberbezpieczny/.

PIONIER-CERT, 'About us'. Accessed December 19, 2016. https://cert.pionier.gov.pl/HomePage.

Polish Financial Supervision Authority, 'Recommendation D On the Management of Information Technology and ICT Environment Security at Banks'. Accessed December 18, 2016. https://www.knf.gov.pl/Images/RecommendationD_tcm75-44254.pdf.

Powstaje Polska Obywatelska Cyberarmia. Accessed November 7, 2016. https://www.cybsecurity.org/powstaje-polska-obywatelska-cyberobrona/.

Research and Academic Computer Network, 'About NASK', Accessed December 18, 2016. http://eng.nask.pl/en/about-nask/about-nask/250,Research-and-Academic-Computer-Network.html.

Responsibilities of the inspector general for personal data protection. Accessed December 18, 2016. http://www.giodo.gov.pl/138/id_art/368/j/en/.

Rynek e-commerce w Polsce – specyfika, trendy, praca. Accessed October 1, 2016. http://www.rp.pl/Biznes/160619670-RYNEK-E-COMMERCE-W-POLSCE--specyfika-trendy-praca.html.

Służba Kontrwywiadu Wojskowego, ‘About MCS’. Accessed November 7, 2016. http://www.skw.gov.pl/en/o-skw.html

Służba Kontrwywiadu Wojskowego, ‘Zadania SKW’. Accessed November 7, 2016. http://www.skw.gov.pl/en/zadania.html.

Śledziewska, Katarzyna, Zięba Damian, ‘E-administracja w Polsce na tle Unii Europejskiej. Jak z niej (nie) korzystamy’, http://www.delab.uw.edu.pl/wp-content/uploads/2016/10/DELab_e-administracja_w_PL.pdf, 2016.

Świątkowska, Joanna, Szwiec, Magdalena., Llacayo, Ana-Isabel. ‘Make a Bomb in the Kitchen of Your Mom – How Terrorists Use Cyberspace and How to Fight with Them’, The Kosciuszko Institute Policy Brief, 2016.

Świątkowska, Joanna, ‘Cyber Security in Poland’, in: ‘V4 Cooperation in Ensuring Cyber Security – Analysis and Recommendations’, Świątkowska, Joanna. (edit.), The Kosciuszko Institute, 2012.

Świątkowska, Joanna (edit.), ‘Critical Infrastructure Security – the ICT Dimension’, The Kosciuszko Institute, 2014.

Umowa PSE-NATO ws. ochrony infrastruktury elektroenergetycznej. Accessed November 7, 2016. http://www.pap.pl/aktualnosci/news,536936,umowa-pse-nato-ws-ochrony-infrastruktury-elektroenergetycznej.html

Wartość rynku e-commerce to 32-33 mld zł. Accessed October 12, 2016. http://www.dlahandlu.pl/handel-wielkopowierzchniowy/wiadomosci/wartosc-rynku-e-commerce-to-32-33-mld-zl,49646.html.

Zieliński, Krzysztof, presentation at 24th International Defence Industry Exhibition MSPO in Kielce, 6-9 September, 2016.

Zwalczaj cyberprzestępczość, Accessed December 18, 2016, http://www.policja.pl/pol/zwalczaj-cyberprzestep/83643,Zwalczaj-cyberprzestepczosc.html.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu