The Entities and Institutions in Charge of Combating Cybercrime in Poland

Jerzy Kosiński

Abstract This chapter presents the relationship between cybersecurity and national and internal security and identifies the effects of cybercrime and the need to combat it. The author, pointing to selected main state institutions and authorities, describes their activities in ensuring cybersecurity and combating cybercrime.

1 Introduction

Cybersecurity is most often understood as the security of globally connected information systems (e.g. the Internet infrastructure), telecommunications networks, computer systems, and industrial control systems. Cybersecurity breaches can serve the purpose of numerous criminal acts which cause substantial financial and non-financial losses for organisations, businesses, and individuals. It is hardly questionable that this problem is also significant in the context of internal security, and, hence, national security.

In 2003, Dan Verton wrote that the uninterrupted functioning of cyberspace¹ in highly developed countries was fundamental, not only for the proper functioning of the economy, but also for national security.² This statement, concerning both external and internal security, has become even more pertinent with the development of information and communication technologies.

¹The emergence of cyberspace is connected with the establishing of the political concept of “the information superhighway” during Bill Clinton’s presidential campaign in 1992, defined as all types of information containing text, sounds, and images, which could be transferred over large distances, in a quick and uninhibited manner. However, it is to Vice President Al Gore to whom greater credit in this field should be attributed, as he continued to promote the development of the information superhighway later during Clinton’s presidency. It is worth noting that the technical and functional concepts of the information superhighway derive from the Infostrada concept proposed in the early 1970s by Prof. Andrzej Targowski.

²Verton (2004), p. 76.

J. Kosiński (✉)

Akademia Marynarki Wojennej w Gdyni/Polish Naval Academy in Gdynia, Gdynia, Poland

e-mail: j.kosinski@amw.gdynia.pl

The rapid technological advancement observed in recent years, and in particular the development of telecommunication technologies and the progressing computerisation in virtually every sphere of human life, have made information the most precious resource. Information is the key to success in politics and business, and in the planning and conducting of military operations. It is no less significant to note that the uninterrupted flow of, and access to, information is indispensable for the proper functioning of the economy, administration, and specialised forces of every country.³

No elements in national power are free from, or independent of, information. The Army, the Police, the financial system, the economy, transportation, energy, healthcare, and the media—all these rely on the functioning of communication and information systems. Information contained and processed in such systems should be protected, as is done with every material good. Information has become the object of conflicts, the tools for which include any means adjusted to its collection, disruption, and protection. Information warfare is aimed at obtaining and using the kind of information resources which contain classified, confidential, and inaccessible information. While it is frequently conducted with a view to gaining access to personal data, it sometimes involves competing businesses and corporations. Information warfare also takes place at the national and regional levels.⁴

The information warfare concept can be approached by analysing its major elements, i.e. information resources and antagonists, as well as offensive and defensive operations.⁵ One of the domains of information warfare includes crimes⁶ which are usually perpetrated, together with Open Source Intelligence (OSINT), and competitive intelligence, for the purpose of offensive operations, while combating cybercrime is among the major duties of governments as regards defensive operations.

What is specific to the threats emerging from the use of ICTs is the absence of physical contact with the perpetrator. The fact that there is no clearly defined adversary makes the threats seem blurred, and less real, which triggers an imminent need to develop and maintain an appropriate security system. The lack of universal social understanding in this field is also a threat in itself, as it hinders reasonable efforts leading to the shaping of cybersecurity space in a multidimensional, concurrent and substantively consistent manner.⁷

It is worth noting that constructing an absolutely secure communication and information system is practically impossible from the technical point of view. Threats to communication and information systems can involve both technological and human factors. On the one hand, threats posed by technology, such as hard drive

³*The White Book on the National Security of the Republic of Poland*, National Security Bureau (BBN), Warsaw 2013, p. 63.

⁴Cf. Ciborowski (2001), p. 9.

⁵More information in Denning (2002), pp. 23–48.

⁶Denning (2002), p. 59.

⁷Ciborowski (2001), pp. 178–179.

failure, are usually foreseeable, and can be properly mitigated (e.g. by doubling the critical system elements), or a desirable level of security can be ensured through risk analysis (e.g. by incremental backups). Threats induced by humans, on the other hand, are much harder to foresee. An attacker might be an outsider in breach of security, or an insider, i.e. a person from within the organisation whose conduct gives rise to a threat. Although the media are much more inclined to publicise information on outsider attacks, various research and analyses have indicated that insider attacks (i.e. perpetrated by current or former employees, contractors, or other business partners) are in fact more dangerous and cause more severe losses.⁸

The Council of the European Union, in its conclusions of 2013 on setting the EU priorities for the fight against serious and organised crime between 2014 and 2017,⁹ recognised as one of its priorities combating cybercrime committed by organised criminal groups and generating large criminal profits, such as online and payment card fraud, cybercrimes which cause serious harm to their victims, such as online child sexual exploitation, and cyber attacks which affect critical infrastructure and information systems in the EU. In 2017, the Council decided to continue the series of EU policy on serious and organised international crime in 2018–2021.¹⁰ Also, it should be borne in mind that the previously adopted Cybersecurity Strategy of the European Union¹¹ emphasised the need to increase the operational capability for combating cybercrime and increasing IT infrastructure's resilience. Based on the same document, a comprehensive approach to the cybersecurity problem should combine three pillars—network and information security, law enforcement, and defence—which are also governed by various legal frameworks.

The scale of cybercrime also appears alarming, with 378 million victims per year, which corresponds to 12 people falling victim to cybercriminals every second. In 2017, cybercriminals stole \$172 billion from 978 million victims in 20 countries. Although the average direct loss dropped to USD 142/victim, cybercrime consequences took on average nearly 24 h (which equals 3 full working days) to be removed. In the United States alone, 143 million consumers have fallen victim to cybercrime, which accounts for over 50% of the adult U.S. population present online.¹²

⁸Increase in Insider Threat Cases Highlight Significant Risks to Business Networks and Proprietary Information, <http://www.ic3.gov/media/2014/140923.aspx>, Survey: More Attacks Coming From Outsiders, Insider Attacks More Costly, <http://www.securityweek.com/survey-more-attacks-coming-outsiders-insider-attacks-more-costly> and Lynch (2006). Accessed on 1 December 2020.

⁹Council conclusions on setting the EU's priorities for the fight against serious and organised crime between 2014 and 2017. Doc 137401/13.

¹⁰<https://www.consilium.europa.eu/pl/policies/eu-fight-against-organised-crime-2018-2021/>. Accessed on 1 December 2020.

¹¹Communication to the European Parliament, the Council, the Economic and Social Committee, and the Committee of the Regions, of 7 February 2013 *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, doc. JOIN (2013)1.

¹²<https://us.norton.com/cyber-security-insights-2017>. Accessed on 1 December 2020.

In testifying before the U.S. Congress on 20 March 2009, Edward Amoroso, CSO of AT&T, estimated that the annual profits made by cybercriminals exceeded \$1 trillion (10^{12}), i.e. more than the revenue generated by the entire IT industry, and corresponding to approximately 7% of the U.S. GDP.¹³ This value, however, might have been overestimated, as it was quoted in connection with applying for financial aid.

Based on the survey conducted by the British Department for Business, Innovation & Skills, in collaboration with PwC, the level of costs incurred by British entrepreneurs due to cybersecurity breaches has reached billions of pounds per year, and these costs have tripled since 2012.¹⁴ The same survey revealed that 87% of small enterprises and 93% of large organisations recorded at least one security breach in 2012. The most severe breaches of cybersecurity cost small enterprises an average of £50,000, and large enterprises (with more than 250 employees) approximately £650,000. To get the bigger picture, these costs should be added to the expenditures on cybersecurity, accounting for approximately 10% of the total IT costs in enterprises. In 2013, for the above reasons, the British Government launched a special CISP¹⁵ platform, comprising officers of the GCHQ,¹⁶ the NCA,¹⁷ MI5, UK CERT, and representatives of business circles (at first from critical infrastructure sectors—defence, energy, finance, pharmaceuticals, and telecommunications), to defend companies against the growing threat of cyber attacks from China, Russia, and Iran.

Although most cyber attacks were outsider violations performed by criminals, hackers, or competitors, internal threats were also reported. 36% of the most severe security breach cases were caused by unintentional human behaviour, and another 10% resulted from systems' being deliberately abused by employees.

Khoo Boon Hui, President of Interpol, at the 41st European Regional Conference,¹⁸ quoted an academic study by the London Metropolitan University, which found “80 per cent of crime committed online is now connected with organised gangs operating across borders.” He also remarked that “the cost of cybercrime is larger than the combined cost of cocaine, marijuana, and heroin trafficking. In Europe, the cost of cybercrime has apparently reached 750 billion Euros a year,

¹³National Research Council. Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. Washington, DC: The National Academies Press, 2010, p. 8, http://www.nap.edu/download.php?record_id=12997. Accessed on 1 December 2020.

¹⁴<http://www.ft.com/intl/cms/s/0/bb3fcc90-ab4a-11e2-ac71-00144feabdc0.html#axzz2RO-fLvvgZ>. Accessed on 1 December 2020.

¹⁵The Cyber Security Information Sharing Partnership, <https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security>. Accessed on 1 December 2020.

¹⁶Government Communications Headquarters.

¹⁷The National Crime Agency.

¹⁸<http://www.interpol.int/content/download/14086/99246/version/1/file/41ER-Khoo-Open-ing-Speech.pdf>. Accessed on 1 December 2020.

[. . .] with US banks purportedly losing \$900 million to bank robbers but \$12 billion to cyber criminals [in 2011].” Perhaps, this was not a landmark finding, considering that Valerie McNevin, an advisor to the U.S. Treasury International Technical Assistance Office, estimated earlier (in 2005) that the global revenue from e-crime had exceeded USD 105 billion in 2004. The proceeds from illegal drug trafficking in the corresponding period had been lower,¹⁹ though better documented. In 2012, the Federal Bureau of Investigation (FBI) recorded a decrease in “physical crime”, including bank robbery, which was in contrast to cybercrime, which had been growing at an alarming rate.²⁰

General Keith Alexander, Director of the U.S. National Security Agency supervising the U.S. Cyber Command, warned in July 2012 that illicit cyberspace activities essentially amounted to “the greatest transfer of wealth in history²¹”. The UNODC report of 2010 revealed that the annual revenue of criminals from identity theft (being the most profitable cybercrime) amounted to \$ 1 billion, and from child pornography to \$ 250 million.²² In the 2012 survey by McAfee, it was estimated that the global cost of cybersecurity amounted to \$ 1 trillion.²³ Obviously, any such findings, especially when they concern phenomena which are hard to measure, such as the cost of cybercrime, should be approached with caution.²⁴ However, even if its level were 50% lower, it would still be a huge sum. In the 2014 report, McAfee analysts stated that the Internet generated \$2–3 trillion in revenue in the global economy per year (with a steady upward trend), but that value was, in fact, reduced by 15–20% due to cybercrime.²⁵

More and more frequently, cybercrime can be treated as a sort of type of “service” rendered by criminals. In simple terms, there are four categories of “services” rendered by the Internet’s criminal underworld:

¹⁹<http://news.techworld.com/security/4881/cybercrime-more-profitable-than-drugs>. This finding has been questioned several times, e.g. <http://www.informationweek.com/experts-debate-whether-cybercrime-profits-surpass-drug-trafficking/d/d-id/1038656?>. Accessed on 1 December 2020.

²⁰<http://www.wmbfnews.com/story/20972727/robberies-decrease-as-cyber-crime-increases-fbi-says>. Accessed on 1 December 2020.

²¹<http://www.ibtimes.com/americas-top-cyberwarrior-says-cyberattacks-cost-250-billion-year-722559>. Accessed on 1 December 2020.

²²The TOCTA 2010 Report, UNODC, pp. 205, 211, <https://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf>. Accessed on 1 December 2020.

²³<http://truth-out.org/news/item/10700-does-cybercrime-really-cost-1-trillion>. This value, however, is often questioned. Further details on the calculation method can be found in a report entitled *The Economic Impact of Cybercrime and Cyber Espionage*, McAfee 2013, <http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf>. Accessed on 1 December 2020.

²⁴The cybercrime cost estimation method can be found in D. Florencio, C. Herley, Sex, Lies, and Cyber-crime Surveys, MSR-TR-2011-75, June 2011, <http://research.microsoft.com/pubs/149886/sexliesandcybercrimesurvey.pdf>. Accessed on 1 December 2020.

²⁵Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II, McAfee 2014. http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf. Accessed on 1 December 2020.

- (1) *Research-as-a-Service*—some criminal groups specialise in facilitating the sales of vulnerabilities on the black market, before modifications to mitigate such vulnerabilities are published by their producers (*zero-day vulnerabilities*). There are also people who act as intermediaries in the sales of this specific kind of intellectual property. Contrary to the other three categories, research as a Service does not necessarily come from illegal sources.
- (2) *Crimeware-as-a-Service*—this category features the “service” of creating and developing malicious software which is aimed at exploiting programming errors, and then using them for specific criminal acts, as well as developing auxiliary software to foster an attack (downloaders, keyloggers, bots, etc.), tools to disguise malicious software with some security mechanisms (keypads, obfuscators, polymorphic malware, etc.), and spam tools. In addition, it can also include creating hardware to be used for data acquisition (e.g. magnetic card skimmers) or security breaking devices (e.g. antennae, eavesdropping devices);
- (3) *Cybercrime Infrastructure-as-a-Service*—this involves the situation in which other cybercriminals can use a set of tools, once developed, against their victims. An example is renting a computer network for perpetrating an attack, as well as providing access to an online platform for the purpose of independently configuring cybercrime tools, or maintaining a platform facilitating the acquisition or exchange of tools enabling criminal activity.
- (4) *Hacking-as-a-Service*—this involves the complete outsourcing of an attack. In this case, the person ordering the service does not need to have any technical expertise. However, this service can cost more than purchasing tools and conducting an attack independently. This category also covers such services as providing information to be used for identity theft, and acquiring credit card data and website login details.²⁶

Another problem arises from the fact that politicians, law enforcement authorities, and the judiciary underestimate the scale of computer-crime threats, and its associations with business. The social costs of cybercrime are frequently neglected, as the focus is only on the financial impact. In addition, the real extent of cybercrime is hard to determine, which largely stems from the fact that such crimes are often revealed accidentally, mainly due to errors made by the perpetrators themselves. Police statistics usually include only those crimes which have been identified. While the Police authorities tend to proudly publicise the numbers of detected crimes, they are reluctant to mention that approximately 70% of these are crimes whose perpetrators were already known at the time of the crime’s detection²⁷ (e.g. they had been identified by the victim or the victim’s services).

²⁶Cf. a report entitled *Cybercrime Exposed. Cybercrime-as-a-Service*, McAfee 2013, p. 3, <http://www.mcafee.com/uk/resources/white-papers/wp-cybercrime-exposed.pdf>. Accessed on 1 December 2020.

²⁷This is the author’s own study of computer fraud in Poland (Adamski and Kosiński 2007, pp. 131–149), but the results in other countries are similar.

The Republic of Poland has a centralised cyberspace-protection system. The responsibilities regarding cybersecurity are shared, *inter alia*, by the Ministry of Digital Affairs, the Ministry of Interior and Administration, the Ministry of National Defence, the Ministry of Justice, the Government Centre for Security, the Office of Electronic Communications, the Inspector General for Personal Data Protection, the Ministry of Economic Development, the Ministry of Foreign Affairs, the Internal Security Agency, the Police, the Intelligence Service, the Military Counterintelligence Service, and the National Bank of Poland, as well as CERT POLSKA, forming part of the Research and Academic Computer Network (NASK).

This study, rather than providing a detailed description of the responsibilities assigned to all these entities, focuses on combating cybercrime, and on briefly outlining the responsibilities of those entities with whom law enforcement engage in close cooperation.

2 The Ministry Competent for Computerisation

Let us begin by outlining and presenting the responsibilities of the ministry competent for computerisation, as it is a single central public institution, responsible for both cybersecurity policy and cybersecurity itself. The ministry competent for computerisation is in charge of the political and strategic coordination of cyberspace to guarantee Poland's security. Duties in this field include establishing the minimum ICT-security requirements in public administration, and defining the minimum requirements for public records and electronic information exchange, as well as the minimum requirements for communication and information systems (based on the Act of 2005 on the Computerisation of the Operations of the Entities Performing Public Tasks, and the Regulation of the Council of Ministers of 2012 on National Interoperability Frameworks). In addition, the ministry of competent for computerisation has also been entrusted with supervising the Office of Electronic Communication, to which telecommunications operators report major incidents regarding telecommunication networks (in compliance with the Act of 2004—Telecommunications Law). The Ministry also supervises the activities pursued by the Research and Academic Computer Network, as a research institute, and as a data-transmission network operator, and the National Cybersecurity Centre (NC Cyber NASK), established in July 2016 as a major centre in charge of the cybersecurity of the Republic of Poland. NC Cyber NASK has been separated, in organisational terms, from the Research and Academic Computer Network's structure. Some of its duties have been delegated to other sections of that research institute. Dyżurnet.pl is one of the NC Cyber NASK divisions, which acts as a point of contact responding to reports received from Internet users about potentially illegal material (mainly related to the sexual abuse of children, and child pornography, but also to acts of aggression for racist, ethnic, religious, and other motives). Another major duty of NC Cyber NASK is to conduct the ongoing monitoring of network threats such as botnets, and of the working methods of their owners.

3 The Internal Security Agency

The Internal Security Agency (ISA) is another public administration authority dealing with cybersecurity as well as cybercrime. The ISA's activities relating to cyber threats focus on coordinating responses to incidents threatening the security of communication and information systems and networks used by state authorities (the duty of CERT.GOV.PL), as well as on developing the capabilities of public administration for protecting ICT resources, and on supervising the early warning system of threats to public administration networks (ARAKIS-GOV). Another of the ISA's activities is to combat cyberterrorism (illegal attacks or threats of attacks on computers, networks, or information systems, resulting from the activities of terrorist groups or foreign intelligence services).

The ISA is mainly in charge of recognising, preventing, and combating threats to the country's internal security and its constitutional order, and in particular to the sovereignty and international standing, independence, and integrity of its territory, and defence. The ISA may collect any personal data (including classified information), and also so-called sensitive data, where justified by the character of the implemented tasks. The ISA has the right to use both such data and information obtained through investigative operations undertaken by authorised bodies, services, and public institutions, and to process such data and information, in compliance with the Act on Personal Data Protection, without the knowledge and consent of the data subjects. If any information or materials obtained through the activities of the bodies, services, or institutions authorised to perform investigative operations indicate that the case constituting the subject matter of such activities falls within the scope of the ISA's duties, these bodies, services, or institutions shall obligatorily transfer the obtained information and materials to the Agency. If, however, any information and materials obtained through the ISA's activities indicate that the case constituting their subject matter falls within the scope of duties of other authorities, services, or institutions, the ISA's Head shall transfer the obtained information and materials to the authorised body, service or institution.

On 1 February 2008, the Governmental Computer Security Incident Response Team (CERT.GOV.PL) was established within the ISA's structure, to ensure and develop the capabilities of public administration units regarding protection from cyber threats, and in particular from attacks on infrastructures comprising information systems and networks, the destruction or disruption of which can severely threaten the lives and health of the country's population, national heritage, or environment, or can lead to substantial financial losses, or obstruct the functioning of public sector entities. In compliance with the CERT.GOV.PL policy, it essentially acts as a computer security incident response team in the domain of government administration. The principal duty of CERT.GOV.PL is to carry out operations related to the security of the information systems of state bodies. This involves ensuring and developing the capabilities of public administration authorities to protect themselves from cyber threats, and in particular from attacks on ICT infrastructure. CERT.GOV.PL mainly deals with cyber incidents in the public sector, and

its duties include coordinating the response to incidents, and handling and analysing incidents, as well as coordinating the response to security breaches. In the case of incidents with a wide spectrum of impacts, CERT.GOV.PL coordinates the measures taken in connection with a given incident and responds to it, and also exchanges information with the entities directly affected by the cyber attack. It also uses the experience gathered from previous incidents, prepares warnings containing technical information and recommendations for further measures, and supplies them to government administration units. This process is aimed at preventing similar attacks on other institutions, or at reducing the likelihood of their occurrence.

4 The Police

Preparatory proceedings in cybercrime cases are conducted by the Police, and are governed by the Act on the Police.

In October 2014, the Department for Fighting Cybercrime was established within the Criminal Office of the National Police Headquarters. Its activities were supported by the Departments for Fighting Cybercrime operating within individual Provincial Police Headquarters. Similar departments were also established in the Capital Police Headquarters in Warsaw, and in the Central Bureau of Investigation. In December 2016, the Department for Fighting Cybercrime operating within the National Police Headquarters was transformed into the Office for Fighting Cybercrime.

The OFC is primarily in charge of implementing activities related to creating the conditions for the effective detection of crimes perpetrated with the use of advanced communication and information technologies. Its duties include, in particular, supervising, coordinating, and supporting activities undertaken by the Departments for Fighting Cybercrime operating within individual Provincial Police Headquarters, and performing investigative operations. These duties are implemented in cooperation with government administration authorities, the courts, public prosecutor's offices, public institutions dealing with cybersecurity, and private entities operating in that field. The following units operate within the Office: the Operations Department, the Investigative Department (including the 24/7 Service Division), the Investigation and Analysis Department, the Support and Research Department, and the General Affairs Department.²⁸

Notably, the fact that the Office's activities were limited to investigative operations was a drawback of the described structure. While undoubtedly these activities are extremely important in the fight against cybercrime, this rather narrow formulation of the Office's responsibilities has some serious implications.

²⁸ <http://bip.kgp.policja.gov.pl/kgp/struktura-organizacyjn/22759,STRUKTURA-ORGANIZACYJNA-KOMENDY-GLOWNEJ-POLICJI.html>. Accessed on 1 December 2020.

Ultimately, the Office's activities frequently result in drawing up a notification of a crime, which, together with the gathered intelligence, is lodged with the police unit or public prosecutor's office with appropriate territorial jurisdiction, with a view to instituting the relevant preparatory proceedings. At the Police, it is often assigned to an officer who has a limited knowledge of cybercrime. This significantly affects the course of the preparatory proceedings at the initial stage, which is when there should be the collection and securing of evidentiary material, which is then handed over to the public prosecutor, and, eventually, to the court. The fact that no Police officers from the criminal investigation division were from the outset expressly delegated to conducting preparatory proceedings related to cybercrime had a negative impact on the quality of the handling of cases in this field. Fortunately, this approach was modified in 2018, and, since then, both the Office and the Departments for Fighting Cybercrime have conducted (inquiry and investigation) proceedings.

It is worth mentioning that in June 2017 the State Public Prosecutor's Office, jointly with the Research and Academic Computer Network, conducted training aimed at identifying the potential systemic, organisational, and legislative barriers which were negatively influencing the pace of proceedings in the event of incidents (cybercrime), thus making it difficult to hold the perpetrators of such acts accountable. The training was attended by representatives of the State Public Prosecutor's Office, the Provincial Public Prosecutor's Office in Warsaw, the Office for Fighting Cybercrime operating within the National Police Headquarters, NC Cyber NASK, and the Research and Academic Computer Network.

As brought to light by the training, the major identified problem which inhibited incident handling, and thus affected the further course of the preparatory proceedings, was the need to precisely determine the appropriate unit or organisational section of the Police to be in charge of conducting procedural activities related to the identified incident. A major finding was also that the officers of the Regional, District and Municipal Police Headquarters, i.e. those units to which cases are handed over once proceedings begin, did not have specialised knowledge of cybercrime, and, in particular, knowledge of the methods and techniques for securing evidence in this field. Those officers also usually lacked the specialised IT tools which would let them effectively, and in particular quickly, conduct activities at the preliminary stage of the preparatory proceedings. Notably, the above-mentioned police units were also overloaded with other criminal cases which they were handling at any given time. Finally, it should be borne in mind that the Police collaborate directly with EUROPOL and INTERPOL, and in cybercrime cases such cooperation is an absolute necessity.

5 The Public Prosecutor's Office

It seems that the Prosecutor's Office is the most important element in combating cybercrime, as the preparatory proceedings in cybercrime cases are either conducted or supervised by Public Prosecutors. However, the common organisational units of

the Prosecution Service generally lack a uniform structure dedicated to fighting against this type of crime.

The former General Public Prosecutor's Office, which had operated until June 2016, and was then changed into the State Public Prosecutor's Office, by way of the Act of 28 January 2016 on the Law on Public Prosecutor's Offices,²⁹ had no organisational structure whatsoever dedicated to fighting cybercrime. Within the framework of the General Public Prosecutor's Office, three prosecutors were appointed to deal with this issue, and in particular with handling international issues related to this type of crime.

It was only in the Regulation of the Minister of Justice of 7 April 2016—the internal rules of the common organisational units of the Prosecution Service,³⁰ that the function of the Prosecution Service to combat cybercrime was expressly mentioned. In §21(1)(a) of the Regulation, concerning the role of the Economic Crime Department, the following statement was included: "Supervising and coordinating preparatory proceedings in cases involving serious crimes perpetrated via the Internet, advanced technologies, and computer systems (cybercrime), conducted by regional, provincial and district Public Prosecutor's offices."³¹ This provision should be interpreted as a sign of a change in the Prosecution Service authorities' approach to the issues of cybercrime.

In the same paragraph, and more specifically in Point 4, the need to engage in international cooperation in the field of combating cybercrime, and to prosecute its perpetrators, were recognised, along with the requirement to cooperate with the Polish representation in EUROJUST, as regards the Prosecution Service's activities, and with other international and supranational organisations acting under international agreements, ratified by the Republic of Poland, on combating cybercrime.³²

Moreover, in § 20(1)(b) of the Regulation, the responsibilities of the Organised Crime and Corruption Department were formulated, i.e. "supervising and coordinating preparatory proceedings in cases involving crimes perpetrated via the Internet, advanced technologies, and computer systems, with a national or international reach (organised cybercrime)"³³.

In the same paragraph, and more specifically in Point 6, the necessity to engage in international cooperation in the field of combating organised cybercrime and to prosecute its perpetrators was also recognised, along with the requirement to cooperate with the Polish representation in EUROJUST, as regards the Prosecution Service's activities, and with other international and supranational organisations

²⁹Act of 28 January 2016 of the Law on Public Prosecutor's Offices Consolidated text, Polish Journal of Laws of 2019, item 740, as amended.

³⁰Regulation of the Minister of Justice of 7 April 2016—the internal rules of the common organisational units of the Prosecution Service Consolidated text, Polish Journal of Laws of 2017, item 1206.

³¹The Regulation: The internal rules of the common organisational units of the Prosecution Service.

³²The Regulation: The internal rules of the common organisational units of the Prosecution Service.

³³The Regulation: The internal rules of the common organisational units of the Prosecution Service.

acting under international agreements, ratified by the Republic of Poland, on combating organised cybercrime.

In consequence of formulating the above-mentioned brief of the Economic Crime Department and the Organised Crime and Corruption Department, Chapter 3 of the Internal rules—“The organisational structure and tasks implemented by regional, provincial and district Public Prosecutor’s offices”—envisaged the possibility of establishing new organisational units. In § 27 on regional Public Prosecutor’s offices, and in § 29 on provincial Public Prosecutor’s offices, the possibility of establishing organisational units to deal with conducting and supervising cases involving crimes perpetrated via the Internet, advanced technologies, and computer systems (cybercrime) was anticipated. As regards regional Public Prosecutor’s offices, a condition was made that these should be multi-person cases involving serious crimes.³⁴

Last but not least, the justice system, or the judiciary, should be discussed. Within the courts, there is no organisational structure dedicated to considering cybercrime cases. Nor are there any reliable data on the number of judges with cybercrime expertise, as the Ministry of Justice does not maintain any statistics regarding this matter.

Although the National School of Judiciary and Public Prosecution has for several years organised courses in this field, addressed to judges and judicial assistants, there are no data which would allow us to determine the number of such professionals’ being trained in cybercrime issues. Data on the courts in which the judges train in, and, with expertise on cybercrime issues, currently preside, are also non-existent. These circumstances, in combination with the fact that cases are randomly delegated to various judges’ sections, lead to the conclusion that both the indictments from, and findings of, incidental preparatory proceedings, as well as the requests for temporary detention as regards cybercrime cases, are assigned to individual judges in a random manner.

While the situation in the judiciary is as such, the Ministry of Justice, as an entity supervising the courts in administrative terms, has already become aware of how serious the problem of cybercrime is. Notably, the Ministry of Justice features central information systems of great significance, not only for the judiciary, such as the National Criminal Register, but also for economic transactions, such as the National Court Register, the Electronic Land and Mortgage Register, and the National Registered Pledge Information Retrieval System. The Ministry of Justice also acts as the administrator of the information systems used in the courts’ work.

Previously, the responsibilities related to cybercrime prevention and cybersecurity had been implemented by the Computerisation and Court Registers Department, but in June 2017 they were delegated to the newly established Digital Security and Protection Office. Along with the underlying duties related to ensuring the protection of classified information, running the Secret Office, and guaranteeing security, the Office also undertakes activities aimed at supervising the functioning of the

³⁴The Regulation: The internal rules of the common organisational units of the Prosecution Service.

cybersecurity protection system at the Ministry of Justice, and its subsidiary units, which includes detecting and preventing threats to cybersecurity, as well as monitoring and analysing the information security status in the Ministry of Justice cyberspace.³⁵

6 The Ministry of Defence

The Computer Incident Response System (CIRS) of the Ministry of Defence implements tasks in the field of coordinating the processes of preventing, detecting, and responding to computer incidents in the communication and information systems and networks of that Ministry.

The CIRS features a three-level structure which is compliant with NATO's recommendations (the CIRS Coordination Centre, the CIRS Support Centre, which implements tasks consistent with the scope of the responsibilities assigned to CERTs, and the administrators of the communication and information systems of the organisational units and some sections of the Ministry).

The principal activities of the CIRS include coordinating responses to computer incidents, handling and analysing events and incidents, and implementing measures aimed at increasing awareness regarding communication and information security. As part of its activities, the CIRS collaborates with the organisational units and sections of the Ministry of Defence, and with organisations from outside the Ministry, both domestic and international.

In May 2019, following the merger of the National Cryptologic Centre and the Information Technology Inspectorate, the establishment of the Cyberspace Defence Troops was announced. On 1 July 2019, the National Cybersecurity Centre was set up through the consolidation of scattered units of the Ministry of Defence, in charge of cybersecurity, cryptography and ICT. The Cyberspace Defence Troops concept assumes establishing, by 2022, the Polish Command of the Cyberspace Defence Troops, and their achieving of operational readiness by 2024.

7 Summary

The above review of the bodies and institutions in charge of combating cybercrime in Poland demonstrates that certain measures to secure cyberspace and to combat cybercrime are indeed being implemented. Unfortunately, most of these are not planned and systemic measures, and they rarely display the requisite coordination.

³⁵<https://bip.ms.gov.pl/pl/ministerstwo/struktura-organizacyjna/biuro-ochrony-i-bezpieczenstwa-cyfrowego/>. Accessed on 1 of December 2020.

They are often limited-range and stop-gap measures forced by necessary modifications arising from Poland's international obligations.

References

- Adamski A, Kosiński J (2007) Oszustwa internetowe w ocenie polskich I amerykańskich policjantów. *Archiwum kryminologii*. Vol. XXVIII
- Ciborowski L (2001) *Walka informacyjna*. Toruń
- Denning DE (2002) *Wojna informacyjna i bezpieczeństwo informacji*. Warsaw, Chapter 2. Teoria wojny informacyjnej
- Lynch DM (2006) Securing against insider attacks. *Information Security and Risk Management* 11
- Verton D (2004) *Black Ice: niewidzialna groźba cyberterrorizmu*. Warsaw

Jerzy Kosiński dr hab. Eng., the associate professor of the Department of Security Systems at the Polish Naval Academy in Gdynia. Until 2018 he served in the Police, dealing with cybercrime, digital evidence, internet OSInt and infringements of intellectual property on the Internet. The organizer of cyclical international conferences "Technical aspects of ICT crime" (20 editions), which next changed their name to "ICT crime XXI" (2 editions). Author of many publications and speeches at conferences in the field of his scientific specialty. He is a witness expert in the field of computer crime and payment cards from the list of the District Court in Olsztyn. He also conducted trainings in the field of cybercrime for the services of other countries (including Armenia, China, Moldova).

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.