DR PIOTR BURCZANIUK
Cardinal Stefan Wyszyński University in Warsaw | DOI: 10.32041/9788367149761/6

Chapter 6. Pre-Trial Activities of Intelligence Service and Law Enforcement Agencies

6.1. Introduction

This chapter will analyse the pre-trial activities directed at the acquisition of information, relevant from the perspective of criminal law enforcement authorities to carry out activities in the identification and detection of cybercrimes and the prosecution of their perpetrators. The considerations focus on two essential types of these activities. First, security activities related to the functioning of the European and national cybersecurity system and, in particular, the proper cooperation of the participants in this system with law enforcement agencies. Secondly, intelligence gathering activities that national services are authorised to carry out, in the context of the possibility and scope of their use in the fight against cybercrime. A complementary element of the considerations in question will be the analysis of international cooperation in both areas indicated above, conducted between services, in particular within the European Union, which is of fundamental importance in the context of combating cybercrime, which is characterised by its cross-border nature.

The main objective of this analysis is to answer the question of whether the scope of activities belonging to both groups and the international cooperation conducted is sufficient given the nature of the current types of cybercrimes and what are the most significant challenges requiring legislative intervention. In addition to

the main objective indicated in the first paragraph, each part of this analysis sets specific objectives related to the specificity of the issue under consideration.

6.2. Impact of the Cybersecurity System on the Fight Against Cybercrime

This section discusses the relevance of the security measures associated with the functioning of the European and national cybersecurity system for the fight against cybercrime. The starting point for these considerations must be the answer to the question of the interplay and impact of these two, theoretically separate, aspects of cybernetic security, i.e., cybersecurity and cybercrime.

Starting with very general definitions of both terms, it should be pointed out that cybersecurity is fundamentally focused on threat prevention. It refers to actions and measures taken by a broad spectrum of individuals, especially owners and users, to protect ICT[1] from digital threats. Combating cybercrime, on the other hand, focuses on the detection and prosecution, of illegal incidents occurring with or against ICTs by authorised state services and authorities.

Identifying the relationship and mutual interdependencies between these two aspects of cybernetic security seems crucial to ensure the effectiveness of efforts in both areas. This is because it is impossible to effectively identify and combat cybercrimes without the necessary level of expertise in the area of the cybersecurity prevention system. At the same time, it is also impossible to carry out this prevention effectively without knowing the actual methods of the perpetrators of cybercrimes. Cybersecurity and the fight against cybercrime are thus still two different but increasingly interlinked aspects of a single cybernetic security, the protection of which requires coordinated actions and increasingly far-reaching cooperation between those responsible for both areas.

[1] Information and Communication Technology, covering a wide range of technologies including computers, software, networks, the internet and mobile devices.

Starting a legal reflection on the cybersecurity system and its impact on the fight against cybercrime, it should be noted that to date, it has not become the subject of a binding and universally applied normative act. Although numerous activation policies in this area have been put in place by the United Nations, in the end, mainly due to diverging interests, they only led to the creation of soft law standards in the form of resolutions and declarations containing only recommendations addressed to Member States. Also regionally, including within the European Union, a similar regulatory approach prevailed. The situation was only fundamentally changed by the adoption of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union,[2] referred to as the "NIS Directive".

The NIS Directive, as indicated in its Article 1, set as a fundamental objective the achievement of a high common level of security of network and information systems in the European Union to improve the functioning of the internal market. This was to be achieved by taking action in three dimensions: firstly, the introduction of network and information security obligations; secondly, the creation of responsible institutions in all Member States; and thirdly, the definition of rules for cooperation between these institutions at the European level.

In the first aspect, the NIS Directive assumed the introduction of security obligations for two groups of entities. The first included Operators of Essential Services (OES), identified at Member State level, i.e., services essential for the maintenance of critical societal and economic activities, operating in one of the sectors listed in Annex II to the Directive, i.e., energy, transport, banking, financial market infrastructures, healthcare, water supply and digital infrastructures. The second includes the genre-identifiable large Digital Service Providers (DSPs) listed in Annex III, i.e., online trading platforms, search engines and cloud computing services. The obligations imposed on them were essentially based on proper risk management, which is based on conducting an assessment

[2] OJ EU L 2016, No. 194, p. 1.

of the risk and implementing security measures appropriate to its type.[3] The NIS Directive established a lower degree of tolerable risk and thus broader obligations for key service providers, who are to be guided primarily by ensuring the continuity of these services. The means of implementing risk management became the identification, prevention, detection and handling of all incident risks and the mitigation of their impact.[4] One of the primary responsibilities of key service operators and digital service providers was to ensure the security of the networks and information systems they use. The requirements imposed by the Member States in this regard were to be proportionate to the risks associated with the network and information system concerned and were to take into account the state of the art of such measures,[5] with a view to eliminating an excessive financial and administrative burden imposed on such operators. The NIS Directive assumed ex ante measures for key service providers, linked to the certification process, while the requirements were considerably relaxed for digital service providers, with only ex post supervisory measures.

The second aspect is that the NIS Directive imposed obligations on each Member State to set up competent national cybersecurity authorities, covering at least the sectors and services designated by the Directive.[6] The Directive established Two levels of cooperation between these authorities: technical and political/strategic. The first level concerns the establishment of the so-called CSIRT teams,[7] which are responsible for dealing with risks and for undertaking incident-response measures. In accordance with the Directive, such teams shall be established at least in the sectors and services designated by the Directive. The national CSIRTs of the Member States and CSERT-EU were to form a CSIRT network to develop confidence and trust between Member States and to promote rapid and effective

[3] Cf. Recital 44.
[4] Cf. Recital 46.
[5] Cf. Recital 54.
[6] In Poland, the uKSC distinguishes several sectors that are key to the functioning of the State, which are supervised by the competent authorities, i.e. the ministers responsible for individual sectors of the economy.
[7] Computer Security Incident Response Teams.

cooperation. In establishing a system of these teams and entrusting them with the task of reporting serious security incidents, the authors of the Directive saw an opportunity for effective prevention and response. Within the framework of political and strategic cooperation, each Member State was to designate a single point of contact for cybersecurity, responsible for cooperation with other coordination bodies in the EU and with the European Commission,[8] in particular within the so-called Cooperation Group, thus laying the foundation for European cooperation on cybersecurity. In addition, the NIS Directive envisaged the creation of national incident strategies and plans[9] and the established requirements for regular security audits.

The deadline for the implementation of the NIS Directive was 9 May 2018. Poland fulfilled this obligation belatedly by adopting the Act on the National Cybersecurity System on 5 July 2018,[10] which entered into force on 28 August 2018, hereinafter referred to as the "uKSC".

In the context of the main thesis presented in this paper, it should be noted that the NIS Directive does not regulate the substantial aspects of the fight against cybercrime in substance. This aspect of cybernetic security has been referred to in a rather concise manner. Indeed, according to recital 8 of the NIS Directive (and its Article 1(6)), it is without prejudice to the possibility for each Member State to take measures necessary, inter alia, to enable the investigation, detection and prosecution of criminal offences. Its Recital 62 also notes that incidents may result from criminal offences the prevention, investigation and prosecution of which is supported by coordination and cooperation between key service operators, digital service providers, competent authorities and law enforcement authorities. Where it is suspected that an incident is related to serious criminal offences under Union or national law, Member States should encourage key service operators and

[8] In Poland, according to the uKSC, it is run by the minister responsible for cybersecurity.

[9] In Poland, the Resolution No. 125 of the Council of Ministers of 22 October 2019, which was adopted, remains valid. Cybersecurity Strategy of the Republic of Poland for 2019-2024 (M.P. of 2019, item 1037).

[10] Journal of Laws 2022, item 1863.

digital service providers to report serious criminal incidents to the relevant law enforcement authorities. Where appropriate, it is desirable that coordination between competent authorities and law enforcement authorities from different Member States be facilitated through the European Cybercrime Centre (EC3) and through ENISA, as described further below.

The assumptions of the NIS Directive mentioned above are reflected in the uKSC. The provision of Article 40(2) of the SCC is of fundamental importance in this context, according to which CSIRT MON, CSIRT NASK, CSIRT GOV and sectoral cybersecurity teams provide information constituting legally protected secrets, including those constituting company secrets, to law enforcement authorities in connection with an incident that fulfils the constitutive elements of a crime. As pointed out in the Polish legal doctrine:

> Article 40(2) complements Article 34 of the KSC Act, allowing criminal proceedings to be conducted in a situation where an incident is found to constitute a criminal act. The legislator has regulated both the cooperation with law enforcement authorities and the rules of exchange of information with them separately, as Article 2(10) narrowly defines the concept of handling an incident. According to the statutory definition, these are activities that make it possible to detect, classify, analyse, prioritise, take corrective action and limit the effects of an incident. Undoubtedly, this definition does not include notifying law enforcement authorities of an incident or securing digital evidence for ongoing criminal proceedings. By contrast, Article 4(8) of the NIS Directive appears to introduce a broader definition of incident handling, which shall be understood as covering all procedures aimed at detection, analysis, mitigation and response to an incident. The response element may therefore include the notification of a crime and the collection of evidence for subsequent investigation. For this reason, the legislator has imposed an obligation on the CSIRT MON, CSIRT NASK, CSIRT GOV and sectoral cybersecurity

> teams to provide information which is a legally protected secret to law enforcement authorities in connection with an incident which fulfils the constitutive elements of a crime. In turn, these authorities in such situations act on the basis of general provisions.[11]

At the same time, in accordance with Article 38 of the SCS, information processed under the Act shall not be made available if its disclosure would, inter alia, adversely affect the investigation, detection and prosecution of criminal offences.

Thus, on the basis of the regulations cited above, it is evident that both the European and the Polish legislator, while creating the rules of cybersecurity management, assumed an immanent necessity of correlation between two aspects of cybernetic security – cybersecurity and combating cybercrime. This conclusion is also confirmed by an analysis of the content of the Cybersecurity Strategy of the Republic of Poland for the period 2019–2024, issued on the basis of Article 68 of the uKSC, which sets out five specific objectives of the Polish government's policy to strengthen and develop the national cybersecurity system. Under the first specific objective on the development of the national cybersecurity system, it was that the capacity to combat cybercrime, including cyber espionage and terrorist incidents should be increased.

A review of the NIS Directive in the EU, after six years in force, has shown that the wide discretion left to Member States in its implementation has led to significant variation in the types and levels of detail in the obligations imposed on service providers, which had a significant impact on their cross-border activities and thus led to fragmentation of the EU internal market and disrupted its functioning. To address this issue, Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, referred to as "NIS Directive 2", was adopted

[11] P. Drobek, [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, K. Czaplicki, A. Gryszczyńska, G. Szpor (red.), Warszawa 2019, Article 40.

on 14 December 2022. It entered into force on 16 January 2023 and the deadline for its implementation is 17 October 2024. The primary objective of the NIS 2 Directive is, as highlighted in its Recital 5, to eliminate divergences between Member States, in particular by defining minimum rules for the operation of a coordinated regulatory framework, establishing mechanisms for effective cooperation between the responsible authorities in the different Member States, updating the list of sectors and activities subject to cybersecurity obligations and introducing effective remedies and enforcement measures, which are key to the effective enforcement of these obligations.

An analysis of both the recitals of this directive and its individual provisions leads to the general reflection that a significant part of its provisions are the result of practical problems encountered by the cybersecurity system shaped by the NIS Directive. Indeed, NIS 2 implies a number of security solutions directed at threats identified in the cybersecurity system in recent years. Hence, its provisions directly refer to specific types of such threats, which either result from a specific methodology of action of the perpetrators, such as, inter alia, ransomware attacks,[12] or are related to the use of specific types of technological solutions, including, inter alia, the Internet of Things[13] and identifiable solutions, e.g., end-to-end encryption.[14]

The NIS 2 Directive abolishes the existing entity-based distinction between key service operators and digital service providers. Instead, a uniform size criterion will be introduced to include even medium-sized enterprises (in some cases also small and micro enterprises) operating in the sectors or providing the types of services covered by the Directive. These entities will be divided into new categories, i.e., key actors (Annex I sectors: energy, transport, banking, financial market infrastructures, healthcare, drinking water, waste water, digital infrastructures, ICT service management, public administration entities, space) and important actors (Annex II sectors) and qualified according to their size, and importance of their respective sectors or the type of services they provide. As can be seen from the above,

[12] Cf. Recital 54.
[13] Cf. Recital 53.
[14] Cf. Recital 98.

the NIS 2 Directive imposes cybersecurity compliance obligations on entirely new entities, significantly broadening the cybersecurity regime. At the same time, the new regulation emphasises the need for a sectoral approach to cybersecurity, assuming and announcing the introduction of sectoral regulations that take into account the specificity and complexity of a particular sector, shaping tailored risk management measures, incident reporting obligations and oversight and enforcement rules. In this context, it should be noted that the Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector,[15] directly targeted at the financial sector, was adopted at the same time as the NIS 2 Directive.

As far as the area of risk management is concerned, the NIS Directive implies the need to balance the measures applied with the degree of dependence of the entity on networks and information systems, the degree of exposure of the entity to risk and the social and economic impact that a potential incident would have. Such measures are aimed at identifying the risk of incidents (including a special assessment of the security of the supply chain of products[16] and services[17]), preventing, detecting, responding to and recovering from incidents and mitigating their impact.[18] The security of the physical environment of networks and systems must also be considered in the new risk management approach. Therefore, an important methodological basis for the measures to be introduced is to be good market practice, based mainly on the standardisation process, with particular reference to the standards contained in the ISO/IEC 27000 series.[19] The whole risk management process is also to take into account the minimisation of excessive financial and administrative burdens.

The NIS 2 Directive emphasises the importance of so-called cyber hygiene, a set of good practices aimed at ensuring overall safety

[15] OJ EU L 2022, No. 333, p. 1.
[16] Cf. Recital 85.
[17] Cf. Recital 86.
[18] Cf. Recital 78.
[19] Cf. Recital 79.

and security in the event of incidents.[20] At the same time, it draws attention to the NIS 2 Directive's move away from purely reactive measures, based on a system of incident reporting and identification, towards active cyber defence, defined as proactively preventing, detecting, monitoring, analysing and mitigating network security breaches, combined with the use of capabilities deployed within and outside the network under attack. Furthermore, the identification and neutralisation of vulnerabilities in networks and information systems, in particular by their manufacturers or solution providers, is to become the key to the new system. Among other things, civil and criminal liability exemptions of the individuals carrying out vulnerability and information security tests enhance the process of identification of vulnerabilities.

The changes introduced by the EU legislator are part of a new approach to cybersecurity policy, which places the user of the system, regardless of his or her role in the system, rather than the information system (hardware and software), at the centre. In a nutshell, this approach assumes that a system is only as secure as its users are aware of the risks and follow certain procedures. This change in approach is the result of analyses of the scale and types of reported significant and critical incidents, which show that most of them have their origin in human activity, which turns out to be the weakest link in the entire cybersecurity system. This new policy therefore breaks with the original assumption of striving for "perfection" of information systems, focusing instead on the activities of people, organisations and states in cyberspace, aiming to steer them towards behaviour that is considered safe.

Interestingly, the need to change the optics of cybersecurity policy was recognised by the Polish legislator even before the adoption of the NIS 2 Directive, proposing as early as January 2021[21] to replace the existing definition of the term "cybersecurity" covered by the PSC, derived from the NIS Directive, focused on the resilience of the information system and its protection, in favour of a definition covering

[20] Cf. Recital 49 and 89.

[21] Article 1(2)(b) of the Bill of 20 January 2021 amending the Act on the National Cybersecurity System and the Act – Telecommunications Law.

activities necessary to protect information systems, users of such systems and other entities, from cyber threats. He also points out that some of the directional changes currently covered by the NIS 2 Directive were introduced into the Polish legal order even before the implementation of the NIS Directive, e.g., by the Act of 10 June 2016. on anti-terrorist activities,[22] which gave the Internal Security Agency, hereinafter referred to as the "ABW", the tasks of identifying, preventing and detecting threats to the security of the public administration's ICT systems and critical infrastructure, to be carried out through powers to: assess the security of these ICT systems, providing, at the request of the Head of the ABW, information on the construction, functioning and principles of operation of these ICT systems, blocking the availability in an ICT system of specific IT data or ICT services related to a terrorist event, keeping a register of events violating the security of these ICT systems, issuing recommendations to the Head of the ABW with a view to improving the security level of ICT systems. In turn, the PCA itself enabled the ABW to implement the ARAKIS-GOV early warning system for Internet-based threats.

In the context of the main thesis presented in this paper, it should be added that the NIS Directive 2, like the NIS Directive, does not regulate the fight against cybercrime in substance, but the extent of its correlation with this aspect of cybernetic security is much clearer than in the case of the previous Directive. In accordance with recital 107, where it is suspected that an incident is related to serious criminal offences under Union or national law, Member States should encourage key and important players, on the basis of the applicable rules of criminal procedure under Union law, to report serious criminal incidents to the appropriate law enforcement authorities. Where appropriate, and without prejudice to the data protection rules applicable to Europol, it is desirable that coordination between competent authorities and law enforcement agencies from different Member States be facilitated by the European Cybercrime Centre and ENISA. In addition, the NIS Directive 2 notes the need to give

[22] Journal of Laws 2022, item 2632.

law enforcement authorities access to information including, inter alia, domain name registration data.[23]

As can be seen from the analysis of the provisions of the NIS Directive and NIS 2, the EU legislator sees the functional relationship between the cybersecurity system and the issue of combating cybercrime as two pillars of cybernetic security. Indeed, there is a strong logical link between securing ITC systems, and thus the services provided by means of such systems and the information stored in them, and the issue of combating cybercrime, which is often a direct consequence of gaps or deficiencies identified in the security policies of these systems or errors associated with their use. The security of information systems is therefore crucial at the prevention stage, as a mechanism to prevent cyber attacks. An analysis of the statistics[24] of the scope of incidents reported within the cybersecurity system leads to the conclusion that most of them aim to exploit vulnerabilities in the security of information systems, with the consequence of acquiring protected information or infecting the system with malware, which constitutes a criminal offence. Therefore, ensuring the security of information systems is one of the primary measures to prevent cybercrime. The NIS Directive and NIS 2 and the entire system established on their basis, are therefore aimed at enhancing the security of information systems in strategic sectors, which indirectly contributes to reducing the possibility of cyber attacks and thus preventively combating cybercrime.

Undoubtedly, the cybersecurity system, based on the prevention, detection and response to various types of cyber threats, plays a key role in the fight against cybercrime. This role is outlined in two key aspects. First, when the cybersecurity system supports the process of identifying and prosecuting cyber criminals. Secondly, when it neutralises opportunities for perpetrators by eliminating system vulnerabilities previously identified in specific criminal activities. Thus, it can be said that, on the one hand, the cybersecurity system,

[23] Cf. Recital 110.

[24] Raport roczny z działalności CERT Polska – Krajobraz bezpieczeństwa polskiego Internetu w 2021 r., Warszawa 2022; Raport roczny z działalności CERT Polska – Krajobraz bezpieczeństwa polskiego Internetu w 2020 r., Warszawa 2021.

by carrying out monitoring, acquires information on specific incidents and secures the evidence necessary to identify the perpetrator; on the other hand, law enforcement findings on the specific modus operandi of the perpetrators, help to neutralise vulnerabilities in ITC systems and thus act as a preventive measure.

The developments in cybersecurity policy indicated above, focusing on the role and importance of the user of an ITC system and therefore also the potential victim or perpetrator of a crime, lead to the conclusion of an even greater need for convergence between these two aspects of cybernetic security in the near term.

However, it should be borne in mind that this rapprochement may face significant legal and practical problems. The most significant of these seem to relate to the different perspectives of the regulators and the main participants in both aspects on privacy and data protection issues. For, on the one hand, there is a great deal of pressure from law enforcement authorities for companies and institutions, which are also participants in the cybersecurity system, to collect and share more and more of such information with them, justifying this by the need to effectively combat cybercrime, while on the other hand, these companies, often inspired by the fears of their own users regarding the threat to their privacy and freedom, implement far-reaching restrictive measures in this regard. The second aspect is the concern about the use of various modern technologies, such as facial recognition systems, online behaviour monitoring or artificial intelligence algorithms, among others, which, on the one hand, may have a high level of effectiveness in the fight against cybercriminals, but, on the other hand, the mechanism of their operation is based on the collection and aggregation of large amounts of personal data, including sensitive data. It seems that both the EU and national legislators will soon be faced with the need to determine the balance between the needs of law enforcement and fundamental personal rights, led by the right to privacy. The Polish legislator will also face these challenges, inter alia, by undertaking the implementation of the NIS 2 Directive in the near future.

Attention should also be drawn to the challenge of the lack of consistency and harmonisation between different countries and regions in terms of both cybersecurity and cybercrime regulation. Many

companies operate globally, in multiple markets and face the need to comply with different standards and regulations, which can lead to complex and costly compliance processes and often, in situations of apparent contradiction, a lack of implementation. The lack of uniform regulations can therefore clearly hinder cooperation between countries and regions in the fight against cybercrime and in cybersecurity emergencies. The challenges described, therefore, do not take a domestic perspective, but clearly demonstrate, firstly, the need for regional and even global cooperation in the creation of an effective cybersecurity system; secondly, they make its emergence dependent on cooperation with ITC solution providers.

6.3. Types and Scope of Law Enforcement Intelligence Gathering Activities to Combat Cybercrime – Current Status and Challenges

The considerations set out in this part are devoted to intelligence gathering activities carried out by national services, in the context of the possibility of their use in order to obtain information relevant from the perspective of combating cybercrime.

The first element of these considerations is the analysis of the term intelligence gathering (the literal translation of the term used in the Polish legal acts is 'operational and reconnaissance activities') used in the Polish legal acts governing the scope of competence of services to define one of the types of activities they are authorised to perform. The analysis of these acts leads to the conclusion that at present[25] – to a different extent – eleven services are authorised to perform them, including six law enforcement services, i.e., the Police, the Military Police and the Border Guards, the State Protection Service, the National Fiscal Administration, the Prison Service (they have, in principle, investigative and administrative powers); and five services defined as special services, i.e., the Internal Security Agency, the Foreign Intelligence Service, the Military Counterintelligence Service, the Military Intelligence Service and

[25] Status as of 29 May 2023.

the Central Anti-Corruption Bureau (they have in principle, analytical and informative powers. The exceptions are the ABW and the CBA, which also have investigative powers). The indicated types of activities reflect the scope of responsibilities of these services – in the case of law enforcement services, their tasks are focused on preventing crimes and prosecuting their perpetrators, whereas, as far as the in intelligence and security services are concerned, their essential tasks include obtaining and transmitting information.

The introduction of a legal definition of the notion of "operational and reconnaissance activities" was assumed in 2008 by the draft act on intelligence gathering activities, defining them such activities as a set of undertakings, overt and covert, conducted for the three purposes indicated in the draft, which consist, in particular, in obtaining, collecting, processing and checking in an overt and covert manner information about crimes and obtaining documentation, samples and comparative materials in order to reveal or secure evidence of a crime.[26] The works on the draft have not been completed. However, discussion about the need for statutory regulation of these activities has been ongoing, including the presentation of a draft Operational Work Code at a Senate hearing in January 2023, which is "intended to be a kind of instruction manual for the operation of the services".[27] However, incomplete legislative activities on the indicated drafts resulted in a lack of the legal definition of the notion of "intelligence gathering activities" in the Polish legal system. What is more, the other types of activities – investigative, administrative or analytical – do not have such a definition either. This implies the necessity to systematically separate and qualify them on the level of legal doctrine.

The literature on the subject emphasises that intelligence gathering shall be understood as activities of competent state authorities which essentially consist of secret and confidential, extra-procedural

[26] Article 2(1) and (2) of the draft law on operational and reconnaissance activities, online: https://orka.sejm.gov.pl/proc6.nsf/projekty/353_p.htm (accessed on: 29.05.2023).

[27] P. Śmiłowicz, *Kodeks pracy operacyjnej dla służb*, "Gazeta Prawna online", 26 January 2023, https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/8646248, kodeks-pracy-operacyjnej-dla-sluzb-ko.html (accessed on: 01.06.2023).

activities of such services, directed at the performance of their tasks related to the prevention of crime and other negative social phenomena and their combating. Moreover, these activities are generally performed outside the framework of criminal proceedings, although they often serve to fulfil the tasks of ongoing or future criminal proceedings.[28] The extra-procedural mode in which such activities are being carried out also translates into the problem of using such material as evidence in a criminal case.[29] It is clearly emphasised that:

> the results and the course of the activities in question do not have a direct evidentiary effect and, therefore, cannot be directly used in the course of criminal proceedings. However, these activities may determine the areas in which evidence needs to be gathered and may also serve to check evidence that has already been gathered. Mostly these activities serve specific ongoing or future criminal proceedings, often initiated on the basis of their results. They may also be carried out without a direct link to a specific criminal case.[30]

The features indicated above – secrecy, "extra-procedurality", deception – as an acceptable and inherent element of such actions, or their informative role, are the most frequently indicated distinctive features of these actions in the legal literature.[31] In addition, the possibility of interchangeably use of such terms as: "operational work, operational activities, operational activities".[32]

---

[28] Cf. Z. Czeczot, T. Tomaszewski, *Kryminalistyka ogólna*, Toruń 1996, p. 67; J. Widacki (red.), *Kryminalistyka*, Warszawa 1999, p. 110; B. Hołyst, *Kryminalistyka*, Warszawa 2016, p. 47.

[29] Cf. P. Czarnecki, *Czynności operacyjno-rozpoznawcze a postępowanie karne*, "Palestra" 2014, nr 7–8.

[30] E. Wójcik, *Czynności operacyjno-rozpoznawcze i ich rola w zwalczaniu przestępczości zorganizowanej*, https://wspia.eu/media/oojnsacq/44-w%C3%B3jcik.pdf (accessed on: 01.06.2023).

[31] Cf. T. Hanusek, *Kryminalistyka. Zarys wykładu*, Kraków 1996, p. 96.

[32] N. Nowicki, *Normatywne ujęcie czynności operacyjno-rozpoznawczych w aspekcie dowodu nielegalnego*, "Przegląd Bezpieczeństwa Wewnętrznego" 2021, t. 13, nr 24, p. 333.

In the context of the correlation between the different types of activities, in accordance with the doctrine of administrative law, intelligence gathering activities are considered to be activities in carried out in the sphere of administrative law, while investigative activities are, on the other hand, an element of procedural activities that are carried out in the domain of criminal proceedings.[33] Moreover, intelligence gathering activities are not followed by any coercive measures translating into a legal obligation to take part in such activities (or to provide information), which is an immanent feature of investigative activities. Finally, as far as the legislative aspects are concerned, investigative activities are governed by the provisions of the Code of Criminal Proceedings while the intelligence gathering activities stem from the legal provisions defining the powers and scope of competence of the respective services. These distinctions thus make it quite easy to separate intelligence gathering activities from investigative activities.

On the other hand:

> the scope of the concept of administrative activities has not been regulated by the Act of 6 April 1990 on the Police[34] but, contrary to the name, other tasks of law enforcement bodies, apart from purely administrative ones, are also performed within their framework. Undoubtedly, administrative activities include explanatory activities in misdemeanour cases, which perform the detection and evidential function.[35]

Thus, the borderline between intelligence gathering activities and administrative-order activities must be analysed each time, taking into account the manner in which a given – specific – activity is performed.

---

[33] Cf. M. Rudnicka, *Ogólna charakterystyka policji jako formacji uzbrojonej i umundurowanej oraz jej wielowymiarowość*, "De Securitate et Defensione. On Security and Defence" 2016, t. 2, nr 2, p. 169.

[34] Journal of Laws 2023, item 171.

[35] A. Taracha, *Kontrola osobista i przeglądanie zawartości bagażu (art. 15 ust. 1 pkt 5 ustawy o Policji) a ochrona konstytucyjnych praw człowieka*, "Prawo w Działaniu. Sprawy Karne" 2020, t. 41, p. 68.

It should also be emphasised that there is no exhaustive catalogue of intelligence gathering activities. Only the most complex types of them, which entail the most far-reaching interference in the sphere of constitutional rights and freedoms, have been regulated in legal statues. These include, inter alia, operational control, controlled purchase, controlled acceptance or presentation of a material benefit, collection and processing of telecommunications data or HUMINT-related activities (cooperation with natural persons providing intelligence to the services). Other types of intelligence gathering activities are regulated by secret internal regulations of individual services, which specify the ways, methods and forms of their performance.[36] In view of the above, only the activities regulated at the statutory level will be subject to further analysis.

In the context of the above observations, turning to the main thread of the considerations concerning the types and scope intelligence gathering activities carried out by law enforcement agencies in the area of combating cybercrime, their delineation must be done, firstly, by specifying the law enforcement agencies responsible for the fight against cybercrime; and secondly, the specific intelligence gathering powers vested in these agencies, the use of which is linked to the fight against cybercrime.

In the first aspect, an analysis of the statutory competence of the Polish law enforcement authorities leads to the conclusion that the key authorities responsible for combating cybercrime in Poland are the Police and the Internal Security Agency (ABW) and, to a lesser extent, the Military Counterintelligence Service. It should be noted that, as far as the abovementioned services are concerned, only the Police is a service of the so-called law enforcement character (whose tasks relate directly to combating crime), while the remaining services belong to the group of intelligence and security services (which primarily gather the information relevant for the neutralisation of potential threats). Hence, the problem of combating cybercrime remains primarily the domain of the Police, and only then the ABW (in the military area the SKW).

[36] Cf. R. Brzozowski, *Czynności wykonywane przez funkcjonariuszy ABW na tle zadań ABW*, [in:] *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, P. Burczaniuk (red.), p. 157.

This inference is underlined by the fact that, according to the Police Act, its basic tasks include, inter alia, initiating and organising activities aimed at preventing the commission of crimes and offences (preventive function), detecting crimes and offences and prosecuting their perpetrators (investigative function). The tasks of the Police, formulated in this way, establish a presumption of its competence in combating crime, including cybercrime – to the exclusion of possible – defined in an enumerative fashion – jurisdiction of other services. The primary role of the Police in combating cybercrime is reinforced by its organisational structure, in which, since 2022 there is the Central Bureau for Combating Cybercrime (CBZC), which is an organisational unit of the Police, responsible for the performing, at the national level, tasks in the field of identifying and combating crimes committed with the use of an IT system, an ICT system or an ICT network, as well as preventing these crimes, as well as detecting and prosecuting the perpetrators of these crimes and supporting, to the necessary extent, the organisational units of the Police in identifying, preventing and combating these crimes.

In turn, the tasks of the ABW are mainly related to the functioning of the national cybersecurity system and tasks in the area of identification, prevention and detection of threats to the security of information and communication systems of public administration bodies or elements of critical infrastructure, which are significant from the point of view of ensuring continuity of the state's functioning. Taking into account its investigative powers, this organ also remains an important element of the system of combating cybercrime, both when the committed offence is related to a breach of the elements of the indicated cybersecurity system, and when the offence is related to offences against state security remaining within its jurisdiction, in particular espionage, terrorism or unlawful disclosure or use of classified information.

Within the framework of intelligence gathering activities, the Commander of the CBZC, under the Act, is vested with powers identical to those of the Commander-in-Chief of the Police or the Commander of the Central Bureau of Investigation of the Police, including: operational control (Article 19 of the Act on the Police), controlled purchase (Article 19a of the Act on the Police), secret

surveillance of production, movement, storage and turnover of objects of crime (Article 19b of the Police Act), obtaining and using information constituting legally protected secrets (Article 20 of the Police Act) and obtaining data not constituting the content of a telecommunication transmission, postal consignment or transmission within the framework of a service provided electronically (Article 20c of the Police Act). The same powers, although different in their scope, correlated with the ABW, are vested in the Head of the ABW (Articles 27–30 and Article 34 of the Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency).[37]

Turning to the first of these activities, one should start by emphasising that the current regulatory shape of both operational control and the power to obtain telecommunication data is structurally identical for all authorised services, which is a consequence of the uniform implementation in 2016[38] of the Constitutional Court's judgment of 30 July 2014 (ref. K 23/11), which outlined the minimum standards for the statutory regulation of the secret acquisition of information about individuals by public authorities.

Pursuant to this regulation, the operational control is initiated, in the formal sense, by virtue of a decision of a competent district court, upon a written application of a competent Police Commander (including the Commander of the CBZC) or the Head of the ABW, submitted after obtaining a written consent of the Public Prosecutor General. The condition for granting such consent is: firstly, submission of a request concerning one of the enumerated offences (different for the Police and the Internal Security Agency), and secondly, facts and circumstances explaining why other operational measures would prove ineffective or would be useless (which emphasises that the operational control is the measure of last resort as an activity having a strong and far-reaching impact on constitutional rights and civil liberties).

In the case of the Police, the operational control may be ordered, inter alia, in order to prevent, detect and identify perpetrators, as well

[37] Journal of Laws 2023, item 1136.

[38] As of 7 February 2016, by virtue of the Act of 15 January 2016 amending the Police Act and certain other acts (Journal of Laws 2016, item 147).

as obtain and record evidence of intentional criminal offences, prosecuted by public prosecution referred to:

1. in Chapter XXV of the Criminal Code, referred to as "CC" (offences against sexual freedom and morality):
   - Article 200a CC (establishing contact with a minor for the purpose of committing a sexual offence),
   - Article 200b CC (propagation of paedophilic behaviour),
   - the entire catalogue of crimes when the victim is a minor or when the pornographic content referred to in Article 202 CC involves the participation of a minor;
2. in Chapter XXIX of the CC (offences against the activities of state institutions and local self-government) – Article 224a of the CC (false alarm);
3. in Chapter XXXIII of the CC (offences against the protection of information):
   - Article 267 § 1–4 CC (both § 1 concerning unlawful acquisition of information, so-called "computer hacking", and § 2 concerning computer eavesdropping, so-called "sniffing"),
   - Article 268a § 1 and 2 CC (thwarting access to computer data),
   - Article 269 KK (damage to computer data; so-called computer sabotage),
   - Article 269a CC (interference with computer system),
   - Article 269b § 1 KK (manufacture of hacking tools);
4. in Chapter XXXV of the CC (offences against property).
   - Article 279(1) CC (burglary, particularly in the context of cash held in bank accounts).
   - Article 285 § 1 CC (activation of telephone impulses).
   - Article 287 § 1 KK (computer fraud; so-called phishing);
5. in Chapter XXXVI of the CC (offences against economic turnover and property interests in civil law transactions) – Article 299 of the CC (money laundering).

In this context, the scope of application of operational control carried out by the ABW, includes, as regards offences which may be committed with the use of ICT methods and means, the offence of unlawful disclosure or use of classified information (Article 265 KK

and Article 266 KK), espionage (Article 130 KK), terrorism (Article 115 § 20 of the CC) and the catalogue of offences covered by Chapters XXXV of the CC (offences against property), XXXVI of the CC (offences against economic turnover and property interests in civil law transactions – including, inter alia, Article 270 of the CC, i.e., theft of funds, or Article 287 of the CC, i.e., computer fraud) and XXXVII of the CC (offences against trading in money and securities) – with the express proviso that they must harm the economic foundations of the state.

Pursuant to Article 19(3) of the Police Act (Article 27(6) of the ABW and AW Act), the operational control is conducted in secret and consists of:

1. obtaining and recording the content of conversations conducted by technical means, including through telecommunications networks,
2. obtaining and recording images or sound of persons from premises, transportation means or places other than public places,
3. obtaining and recording the content of correspondence, including electronic correspondence,
4. obtaining and recording data contained in computer storage media, telecommunications terminal equipment, information and communication technology systems,
5. gaining access to and controlling the contents of deliveries.

The right to carry out the operational control is mutually correlated with the obligation on the part of a telecommunications entrepreneur, postal operator and service provider providing electronic services to ensure, at their own expense, technical and organisational conditions allowing for carrying out such control (Article 19(12) of the Police Act and Article 27(12) of the ABW and AW Act). Importantly, these obligations are further specified, with regard to the telecommunications entrepreneur in Article 179 of the Act of 16 July 2004. Telecommunications Law[39] and the postal operator in Article 82 of the Act of 23 November 2012 Postal Law.[40] However,

[39] Journal of Laws 2022, item 1648.
[40] Journal of Laws 2022, item 896.

such obligations are not specified with regard to a service provider providing services by electronic means, in the Act of 18 July 2002 on the provision of services by electronic means.[41]

The indicated provisions do not specify the technical aspects of the application of the operational control, which seems to be a conscious will of the legislator, leaving this issue to the services, ensuring the flexibility of their actions in conditions of technological variability. On the other hand, the services are under a legal obligation to protect the means, forms and methods of their operations (Article 20a(1) of the Police Act, Article 35(1) of the ABW and AW Act), "therefore the technical issues related to the implementation of eavesdropping are not the subject of the application for ordering operational control".[42] Therefore, in the Polish legal system, it is not required to directly grant the services the right to use, for example, software called "state trojans" to break through the security of telephones and computers and read the contents of devices used by persons, as is the case, in inter alia, Germany.[43]

The scope of activities falling under the operational control, in particular including the so-called electronic surveillance, undoubtedly remains the most important and effective tool in the hands of law enforcement agencies aimed at combating cybercrime. Indeed, the detection and prosecution of many types of cybercrime is only possible thanks to the ability of authorised services to monitor electronic means of communication, content delivered electronically or, finally, electronic data itself. These activities may include various levels of "depth" of interference in the rights and freedoms of citizens, including in particular the secrecy of correspondence, ranging from the analysis of messages transmitted via e-mail, instant messaging or by internet chats, to the examination of user activity on social networking platforms or information on the websites followed by the user.

---

[41] Journal of Laws 2020, item 344.

[42] P. Opitek, *Kontrola telefonu za pomocą Pegasusa*, "Legalis online", 21 January 2022, https://legalis.pl/kontrola-telefonu-za-pomoca-pegasusa/ (accessed on: 04.06.2023).

[43] Ibid.

It should be added that the effective application of this activity, mainly due to technological development, encounters numerous difficulties. One of the most frequently mentioned issues in the literature on the subject is, in particular, the problem of cooperation, in the course of carrying out operational control, with foreign (not based in Poland) providers of electronic means of communication. While, they are obliged to provide, at their own expense, technical and organisational conditions enabling operational control on the basis of the aforementioned regulations, in practice cooperation with such providers, in particular those based outside the EU, may be illusory and de facto dependent on their good will (and often their own privacy policies). Access to the content of the communication itself, which is currently encrypted for most communicators, remains a separate issue. As emphasised in the literature, on the one hand, the providers themselves do not have the possibility to decrypt the transmitted messages, on the other hand, the possible imposition of such access by legal regulations would entail the necessity to build into these services the so-called backdoors available to the services, which in turn would undermine the sense of the services provided.[44] Finally, the last problem concerns anonymous activities of web users, mainly in the area of the so-called "Darknet" (also known as the "Dark Web"). It is a hidden area of the World Wide Web, not indexed by standard search engines and requiring access through special tools and software, such as anonymous networks and darknet browsers. It appears that the use of other types of operational and exploratory activities, discussed below, would be appropriate to explore and investigate this area of the web. Access to data itself, increasingly processed in the so-called cloud, also remains an important issue. On the one hand, this data is physically located in different parts of the world, while on the other, it remains secured by extensive encryption technology.

[44] Cf. S. Wikariak, *Coraz więcej inwigilacji ze strony służb? Projektowane przepisy budzą kontrowersje*, "Gazeta Prawna online", 24 January 2023, https://www.gazetaprawna.pl/firma-i-prawo/artykuly/8644248,policja-sluzby-kontrola-operacyjna-inwigilacja-dostep-do-danych-komunikatory.html (accessed on: 04.06.2023).

Incidentally, it should be pointed out that the operational control discussed above (which is one of the intelligence gathering activities) should be distinguished from the so-called procedural surveillance, specified in Article 237 of the Code of Criminal Procedure (which is one of the investigative activities), i.e., control and recording of telephone conversations ordered by the court at the prosecutor's request, after the commencement of criminal proceedings, with the aim of detecting and obtaining evidence for the ongoing proceedings or preventing the commission of a new offence.

One of the intelligent gathering activities different from operational control remains the so-called controlled purchase. Pursuant to Article 19a of the Police Act (Article 29 of the ABW and AW Act), the Police Commissioner (in the case of the ABW – the Head of the ABW), after obtaining a written consent of the competent regional public prosecutor (in the case of the ABW – the Public Prosecutor General) may order, for a specified period of time, that activities aimed at verifying previously obtained reliable information on a crime and establishing perpetrators and obtaining evidence of a crime, consisting in the secret acquisition, disposal or seizure of objects originating from a criminal offence, subject to forfeiture, or the manufacture, possession, transportation or circulation of which is prohibited, as well as the acceptance or presentation of a material benefit and the submission of an offer in the indicated scope, be carried out. This activity is referred to as "the controlled purchase" or police provocation. Although the original purpose of this activity was to infiltrate criminal gangs dealing in illegal goods, in particular drugs, alcohol, cigarettes, but also firearms or explosives, there would be no obstacle to its current use to combat cybercrime through, for example, the controlled purchase of copyright-infringing digital goods in the form of illegal software, films, music or e-books, but also stolen confidential data or hacking tools, or even "services" related to cyber attacks. However, while, in the current state of the law, the use of operational control and controlled purchase is possible against the offences specified in Article 267 § 1 KK (computer hacking) or Article 269b § 1 KK (production of hacking tools), these tools may not be used with regard to crimes under Articles 115–117 of the Act of 4 February

1994 on copyright and related rights,[45] i.e., crimes of intellectual theft, due to the fact that they have not been entered into the catalogue specified in Article 19, paragraph 1 of the Police Act. It is reasonable to consider the appropriate amendments in this respect.

Another statutory intelligence gathering activity is the so-called controlled delivery. Pursuant to Article 19b of the Police Act (Article 30 of the ABW and AW Act), the relevant Police Commander (in the case of the ABW – the Head of the ABW), may order secret surveillance of the production, movement, storage and trade in objects of an offence, if this does not create a threat to human life or health. The competent prosecutor (in the case of the ABW – the Prosecutor General) shall be notified immediately that such activities have been initiated. The ABW and AW Act emphasises that this activity, which is always ordered prior to the initiation of criminal proceedings, is intended to document offences falling within the scope of competence of the ABW or to establish the identity of persons participating in them or to seize objects of offences. In practice, this activity consists of deliberately failing to intervene or refraining from immediately arresting a suspect in order to allow further collection of information on criminal activities and identification of other persons related to the crime. Through this activity, a law enforcement agency can supervise or observe criminal suspects, acting in an undercover manner, in order to gain more information and collect evidence of their activities. Covert surveillance may include tracking the movement of criminal items, such as tracking shipments, cars or containers to identify individuals and groups associated with the crime. It may also include the observation of places where items of crime are stored, produced or traded in order to identify suspects and collect evidence of their activities. If carried out effectively, these activities make it possible to identify entire criminal networks and apprehend key individuals responsible for the crime. Traditionally, therefore, this activity has been used to combat traditional forms of crime, mainly organised crime such as drug trafficking. Its use against cybercrime is a more complex issue and, as it seems, practically limited, due to the specific nature

[45] Journal of Laws 2022, item 2509.

of criminal activities in the online environment. This is because, for the most part, cybercriminals, using technological safeguards such as VPNs, operate anonymously, effectively concealing their identities. Moreover, some forms of cybercrime, such as hacking attacks, among others, can be difficult to monitor in real time. However, despite these difficulties, its application in some aspects of fighting cybercrime seems possible, e.g., by creating an appearance that an undercover operative or officer is interested in purchasing certain digital goods on online forums or darknets, in order to gain information on the trafficking of illegal software, data theft or hacking tools. Such activities could also include monitoring criminal activities in cyberspace, such as harassment or blackmail, in order to identify their perpetrators. Despite the actual possibilities, the technical side of these activities will remain a challenge, related not only to having the right skills and tools, but also to working with digital service providers to obtain the necessary information and technical support.

Based on Article 20c of the Police Act (Article 28 of the ABW and AW Act), both the Police and the ABW are entitled to obtain and process data, without the knowledge and consent of the data subject, not constituting the content of, respectively, a telecommunication transmission, a postal consignment or a transmission within an electronically provided service, as defined in:

1. Article 180c and Article 180d of the Telecommunications Act, referred to as "telecommunications data", comprising:
   a) the so-called billing records, i.e. data identifying the network termination point, the telecommunications terminal equipment and the end user originating the call and to whom the call is directed (identifying the date and time of the call, its duration, type of call, location of the telecommunications terminal equipment),
   b) other telecommunications data:
      - covered by telecommunications secrecy in terms of: user data, transmission data, location data, data on attempts to connect between network terminations;
      - processed with the consent of the user who is an individual, other data of that user in connection with

the service provided, in particular bank account or payment card numbers, as well as contact telephone numbers,
- a list of subscribers, users or network termination points, taking into account the data obtained at the conclusion of the contract;

2. Article 82 item 1 point 1 of the Postal Law Act, referred to as "postal data", including data on postal operator, provided postal services and information enabling identification of users of these services;
3. Article 18(1) to (5) of the Provision of Services by Electronic Means Act referred to as "online data", including the surname and forename of the service recipient, PESEL number (or other identity document), permanent residence address, correspondence address and data used to verify the service recipient's electronic signature.

The analysed activity, along with the operational control, is a key tool used to combat cybercrime. Moreover, due to the simplified – in comparison to the operational control – mode of obtaining telecommunication, postal and Internet data, it makes it an essential tool in this area. In particular, is an effective tool in the domain of identifying suspicious activity, enabling the linkage of the individual digital traces provided by such data, leading to the identification of cybercrime perpetrators. In addition, a broader analysis of this data, identifying patterns and anomalies in the use of telecommunications services, can raise suspicion that a cybercrime of particular type has been committed, essentially computer fraud (e.g., a large number of calls or messages may indicate use of bots or other automated tools used by fraudsters) or sexual fraud (e.g., the identification of specific communication patterns may lead to the identification of sexual offenders, in particular grooming or the distribution of child pornography).

It should also be borne in mind that the activities discussed above, consisting in obtaining data at the pre-trial stage, should be distinguished from the instrument of obtaining and securing computer data at the pre-trial stage, as an investigative power provided for in Article 217 of the Code of Criminal Procedure

in conjunction with Article 236a of the Code of Criminal Procedure or 218a of the Code of Criminal Procedure.

It should also be noted that a fundamental political and legal debate is currently taking place around this activity, specifically the scope of telecommunications data collected by operators, at both the European Union and national level. On the one hand, the Court of Justice of the European Union, in a number of rulings questioned the universal, generalised and undifferentiated obligation to retain all traffic and location data of all subscribers and registered users, of all means of electronic communication. Furthermore, in the CJEU's view, access by the competent authorities to the stored data should be subject to prior control by a court or an independent administrative authority. On the other hand, it is pointed out that currently retention obligations are not covered by electronic communication providers (e.g., providers of e-mail and instant messaging services), which creates a significant information gap in this respect. Amendments in this respect were proposed by the Polish legislator in the draft Law on Electronic Communications, which was met with a negative reaction of both public administration bodies (e.g., the Minister for European Union Affairs) and publicists and representatives of social organisations.[46]

In the context of these considerations, it should be added that according to Article 20 of the Police Act (Article 34 of the ABW and AW Act), the Police may process information, including personal data, to the extent necessary for the performance of its statutory tasks. The personal data processed in accordance with this provision may also include information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and include genetic and biometric data for the purpose of uniquely identifying a natural person or data concerning a person's health, sexuality or sexual orientation.

[46] Cf. A. Obem, *Polski rząd wdraża prawo unijne… niezgodnie z prawem unijnym. Służby dostaną więcej danych*, Panoptykon Foundation website, https://panoptykon.org/wiadomosc/pke-prawo-komunikacji-elektronicznej-sluzby-retencja-danych (accessed on: 05.06.2023).

The so-called camouflage, set out in Article 20a of the Police Act (Article 35 of the ABW and AW Act), on the basis of which the Police officers (or, respectively, the ABW officers), while performing intelligence gathering activities, may use public documents or other documents which make it impossible to establish the identification data of a police officer and the means he/she uses to perform the official tasks, constitutes an important instrument supporting the intelligence gathering activities analysed above.

6.4. International Information and Operational Cooperation in the Fight Against Cybercrime

This section considers international cooperation between services, particularly within the European Union, when carrying out pre-trial activities. This cooperation is of fundamental importance in the case of the fight against cyber threats and cybercrime, which are characterised by their cross-border nature.[47]

In this respect, both the Police and the Internal Security Agency are entitled to conduct such cooperation, while its character, resulting from the legal construction, is shaped differently in both services. Pursuant to Article 1(2)(7) of the Police Act, one of the tasks of this service is cooperation with the police of other countries and their international organisations, as well as with bodies and institutions of the European Union on the basis of international agreements and arrangements and separate regulations. In turn, in accordance with Article 8 of the Act on the ABW and AW, the service may undertake cooperation with competent authorities and services of other states, which may take place after obtaining the consent of the Prime Minister.[48] The regulation of the powers of international cooperation of the Police and the ABW, different

[47] The considerations do not include the issue of international procedural cooperation, regulated, inter alia, by the Council of Europe Convention on Cybercrime (OJ EU L 2015, No. 728).

[48] The MP's bill to amend the Act - Criminal Code and certain other acts (print No. 3232) envisages extending the cooperation in question to include an 'international organisation'.

in mode and scope, results from two basic assumptions. In the case of law enforcement services, the need for international cooperation is obvious from the perspective of tasks related to combating crime and results from international obligations. Moreover, it takes place openly and in an institutionalised manner, as exemplified by police cooperation within organisations such as Interpol or Europol. This is not the case, however, with the intelligence and security services, which, as state bodies carrying out information-oriented, and thus by definition secret, activities aimed at protecting the interests of the state, including against the actions of other states. This necessitates a cautious and formalised approach to international cooperation. As it seems, these factors provided the rationale for the introduction of an additional supervisory measure in the form of a consent of the political level conditioning the undertaking of such cooperation by the ABW.[49]

The international cooperation, from the perspective of the many actors involved in this process, can take the form of multilateral (multilateral) or bilateral (bilateral) cooperation.

Multilateral cooperation is mainly conducted under multilateral international treaties, mainly by international organisations, with a clear formal definition of the mandate, objectives and principles of operation, organisational structures and sources of funding. In this context, from the perspective of obtaining information on cyber threats and cybercrime, cooperation within the European Cybercrime Centre (EC3) and within ENISA becomes particularly important for the Polish services. Importantly, as indicated earlier, both the NIS Directive[50] and the NIS Directive 2,[51] explicitly assumed the necessity of the coordination of activities between competent authorities and law enforcement agencies from various EU Member States, using the organisations mentioned above.

[49] Cf. M. Kamiński, *Prawne aspekty współpracy międzynarodowej służb specjalnych*, [in:] *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, P. Burczaniuk (red.), Warszawa 2021, pp. 182–183 and 194.

[50] Cf. Recital 62.

[51] Cf. Recital 110.

EC3 was established by the European Union in 2013 as part of the structures of the European Union Agency for Law Enforcement Cooperation (Europol),[52] to coordinate the fight against cybercrime in the EU, as well as to develop cybercrime tools and training and training materials. The Centre offers operational, strategic, analytical and forensic support to investigations carried out by Member States. In this way, the EC3 has four core functions:

1. serves as the European contact point for information on cybercrime,
2. brings together the expertise on cybercrime available in Europe to build the capacity of Member States to combat this phenomenon,
3. supports national cybercrime investigations,
4. provides law enforcement and judicial services with a collective voice in cybercrime investigations carried out in Europe.

As far as organisational details are concerned, EC3 comprises two divisions:

1. Operations (EC3-Operations), which includes task forces focused on detecting and monitoring criminal activities in areas such as online child sexual abuse, online fraud and cybercrimes against critical infrastructure and key information systems within the EU.
2. management (EC3-Management), which is responsible for the administration of the centre, external contacts and operational support, the development of an operational strategy, as well as the development of investigative skills.[53]

The quality of the EC3's operational activities is directly conditioned by the direct involvement of the Member States and the extent of the data they provide.

As regards strategic aspects, a key role is played by a report entitled EU Serious and Organised Crime Threat Assessment (SOCTA),

[52] Communication from the Commission to the Council and the European Parliament tackling crime in our digital age: establishing a European Cybercrime Centre (COM (2012) 0140 final).

[53] Cf. T. Safjański, *Taktyczno-kryminalistyczne aspekty działania Europejskiego Centrum ds. Walki z Cyberprzestępczością*, "Przegląd Policyjny" 2016, nr 2(122), p. 118.

which is prepared on the basis of national risk assessments that are forwarded to Europol by the Member States.

As far as the exchange of information on cybercrime is concerned, the EC3 uses a dedicated online cybercrime reporting system for this purpose as well as collects information on cybercrime from a wide variety of sources, both public and private. The centre collects information on the activities of cybercriminals, the methods they use, as well as on people suspected of cybercrime. The centre facilitates networking between law enforcement agencies, Computer Emergency Response Teams (CERTs) and private sector ICT security professionals. Importantly, the EC3 provides a focal point for the exchange of information not only between member states, but also with third countries (it has, among other things, a well-developed cooperation with the FBI).

It should be added that in 2014, the EC3 established the Joint Cybercrime Action Taskforce (J-CAT), consisting of a permanent operational team of cyber liaison officers from several EU Member States (including the Polish Police) and non-EU partners.[54] The team conducts intelligence-driven coordinated action against key cybercrime threats and targets by facilitating joint identification, prioritisation, preparation, initiation and execution of cross-border investigations and operations by partners. J-CAT's jurisdiction includes cybernetic crime (understood as crimes that use electronic and digital technology to attack computers or computer networks), international payment fraud, online child sexual exploitation and aiding and abetting cybercrime (bulletproof hosting, anti-virus services, criminal use of the darknet, etc.).

In conclusion, it can be pointed out that the EC3 acts as a kind of European "back office" coordinating and supporting national police authorities in their tasks of fighting cybercrime.

In contrast, the European Union Agency for Cybersecurity (ENISA) has a different role as the core element of the European cybersecurity system. It was established in 2004 as the European Network and Information Security Agency (ENISA) under Regulation

[54] As of 20 June 2023, it includes 12 EU Member States and 7 non-EU partner countries.

(EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004,[55] with its headquarters in Athens. The latest reorganisation of ENISA, including the change of its name to its current name, took place in 2019 on the basis of the Regulation (EU) No. 2019/881 of the European Parliament and of the Council of 17 April 2019.[56] Article 3 of this Regulation equipped ENISA with a mandate to carry out tasks with a view to achieving a high common level of cybersecurity across the Union, including by actively supporting the Union's Member States, institutions, bodies, authorities and entities in improving cybersecurity. This objective is to be achieved mainly through the provision of expertise, technical support and coordination between Member States. According to the fifth objective, covered by Article 4 of the said Regulation, ENISA promotes cooperation, including information sharing and coordination at Union level, among Member States, Union institutions, bodies, offices and agencies and relevant public and private sector stakeholders on issues related to cybersecurity. In this way, it effectively acts as a platform for information sharing and coordination between EU Member States in the event of major cyber incidents. On 27 June 2019, ENISA's statutory body became the Network of National Liaison Officers (NLOs), whose role is to facilitate the exchange of information between ENISA and Member States and to support ENISA in disseminating its activities, findings and recommendations to relevant stakeholders across the Union. With respect to the Polish institutional architecture, the role of the contact point is performed by the director of the CSIRT division of NASK. Importantly, ENISA's new task, in line with the NIS 2 directive, will be to prepare a publicly available database of publicly known vulnerabilities.

As far as the exchange of information within the cybersecurity system is concerned, in addition to ENISA, whose role in this regard is paramount, it is also important to remember:

[55] Its mandate was successively renewed by EU regulations in 2008, 2011 and 2013.

[56] OJ EU L 2019, No. 151, p. 15.

1. The Horizontal Working Party on Cyber Issues (HWPCI), which provides strategic coordination of cybersecurity issues in the EU Council.
2. The NIS Cooperation Group, established by the European Commission's Executive Decision of 1 February 2017 in relation to the implementation of the NIS Directive, whose mission is to support efforts to achieve a high common level of network and information security within the EU. The group consists of representatives of EU Member States, the European Commission and ENISA. Poland is represented by the minister responsible for information technology.
3. The CSIRT network, established under the provisions of the NIS Directive, is responsible for international cooperation at the operational level. The network consists of national CSIRT units. Poland is represented in it by CERT Polska.
4. The European Cyber Security Organisation (ECSO), established in June 2016 to facilitate contractual public-private partnerships in cyberspace between the private sector, the European Commission and the public administrations of the Member States.
5. The Central European Platform for Cybersecurity (CECSP), a regional forum which includes representatives from the Visegrad Group (V4) countries and Austria; the CECSP is where, among other things, cybersecurity strategies are reviewed and the current implementation of the NIS Directive is discussed.

With regard to bilateral cooperation, it should be pointed out that it is mainly based on bilateral international agreements. In accordance with the legal doctrine, such agreements make it possible to regulate in detail the cooperation of authorities and institutions of two countries that have common interests in a given area. In the context of the considerations covered in this chapter, agreements on cooperation in combating crime are of particular importance. They regulate the cooperation of authorities at the pre-trial stage (procedural cooperation is regulated by separate agreements on mutual assistance in criminal matters). An essential element of such agreements is the specification of the catalogue of crimes,

in combating which, the parties to the agreement plan to cooperate In turn, the purpose of these agreements is usually to enable the exchange of information between the authorities of both parties, authorised to combat such offences, indicated in the agreement. However, they often also regulate various forms of operational cooperation, such as covert surveillance or undercover operations. Currently, Poland has concluded 41 such agreements.[57]

An important area of bilateral international cooperation is direct operational and information cooperation between the services, based mainly on mutual trust and common interests.

6.5. Conclusions

The considerations presented in this chapter lead to the fundamental conclusion of the need to consolidate, both at the legislative and practical level, activities aimed at securing cyberspace. It is evident that, both at the level of European and national legislation and at the level of the tasks of services and entities responsible for such security, there is a line of demarcation separating preventive activities (the area of cybersecurity) from information activities aimed at combating threats, to procedural activities strictly related to the fight against cybercrime. This boundary exists not only in the area of doctrinal considerations, but translates directly into the tasks and powers granted to the services in individual areas and entities responsible for them. These tasks and powers are not accompanied by clearly defined coordination rules and cooperation mechanisms. This is all the more incomprehensible in view of the fact that these entities serve to ensure a single cybernetic security, with the only distinction being that their tasks concentrate on its individual phases.

This comprehensive view should be adopted, by both the European and national legislator, in the numerous drafts of normative acts aimed at raising the level of cybersecurity currently under way. An essential part of these considerations should be to coordinate

[57] Internetowa Baza Traktatowa Ministerstwa Spraw Zagranicznych, https://traktaty.msz.gov.pl/umowa-1 (accessed on: 22.06.2023).

the actions of those responsible for these various phases and to implement elements to facilitate cooperation, including in particular cross-border information exchange and actual cooperation in the case where specific security incidents occur.

REFERENCES

Act of 6 April 1990 on the Police (Journal of Laws 2023, item 171).

Act of 4 February 1994 on copyright and related rights (Journal of Laws 2022, item 2509).

Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency (Journal of Laws 2023, item 1136).

Act of 18 July 2002 on the provision of services by electronic means (Journal of Laws 2020, item 344).

Act of 16 July 2004. Telecommunications Law (Journal of Laws 2022, item 1648).

Act of 23 November 2012. Postal Law (Journal of Laws 2022, item 896).

Act of 10 June 2016 on anti-terrorist activities (Journal of Laws 2022, item 2632).

Brzozowski, R., *Czynności wykonywane przez funkcjonariuszy ABW na tle zadań ABW*, [in:] *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, Burczaniuk, P. (red.), Warszawa 2021.

Communication from the Commission to the Council and the European Parliament tackling crime in our digital age: establishing a European Cybercrime Centre (COM (2012) 0140 final).

Czarnecki, P., *Czynności operacyjno-rozpoznawcze a postępowanie karne*, "Palestra" 2014 nr 7–8.

Czeczot, Z., Tomaszewski, T., *Kryminalistyka ogólna*, Toruń 1996.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ EU L 2016, No. 194, p. 1).

Directive (EU) 2016/1148 (OJ EU L 2022, No. 333, p. 80).

Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing

Drobek, P., [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Czaplicki, K., Gryszczyńska, A., Szpor, G. (red.), Warszawa 2019, Article 40.

Hanusek, T., *Kryminalistyka. Zarys wykładu*, Kraków 1996.

Hołyst, B., *Kryminalistyka*, Warszawa 2016.

Kamiński, M., *Prawne aspekty współpracy międzynarodowej służb specjalnych*, [in:] *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, Burczaniuk, P. (red.), Warszawa 2021.

Nowicki, N., *Normatywne ujęcie czynności operacyjno-rozpoznawczych w aspekcie dowodu nielegalnego*, "Przegląd Bezpieczeństwa Wewnętrznego" 2021, t. 13, nr 24.

Obem, A., *Polski rząd wdraża prawo unijne... niezgodnie z prawem unijnym. Służby dostaną więcej danych*, Panoptykon Foundation website, https://panoptykon.org/wiadomosc/pke-prawo-komunikacji-elektronicznej-sluzby-retencja-danych (accessed on: 05.06.2023).

Opitek, P., *Kontrola telefonu za pomocą Pegasusa*, "Legalis online", 21 January 2022, https://legalis.pl/kontrola-telefonu-za-pomoca-pegasusa/ (accessed on: 04.06.2023).

Raport roczny z działalności CERT Polska – Krajobraz bezpieczeństwa polskiego Internetu w 2020 r., Warszawa 2021.

Raport roczny z działalności CERT Polska – Krajobraz bezpieczeństwa polskiego Internetu w 2021 r., Warszawa 2022.

Regulation (EU) No. 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act) (OJ EU L 2019, No. 151, p. 15).

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (OJ EU L 2022, No. 333, p. 1).

Resolution No. 125 of the Council of Ministers of 22 October 2019, which was adopted, remains valid. Cybersecurity Strategy of the Republic of Poland for 2019–2024 (M.P. of 2019, item 1037).

Rudnicka, M., *Ogólna charakterystyka policji jako formacji uzbrojonej i umundurowanej oraz jej wielowymiarowość*, "De Securitate et Defensione. On Security and Defence" 2016, t. 2, nr 2, p. 169.

Safjański, T., *Taktyczno-kryminalistyczne aspekty działania europejskiego centrum ds. Walki z Cyberprzestępczością*, "Przegląd Policyjny" 2016, nr 2(122), p. 118.

Śmiłowicz, P., *Kodeks pracy operacyjnej dla służb*, "Gazeta Prawna online", 26 January 2023, https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/8646248,kodeks-pracy-operacyjnej-dla-sluzb-ko.html (accessed on: 01.06.2023).

Taracha, A., *Kontrola osobista i przeglądanie zawartości bagażu (art. 15 ust. 1 pkt 5 ustawy o Policji) a ochrona konstytucyjnych praw człowieka*, „Prawo w Działaniu. Sprawy Karne" 2020, t. 41.

Widacki, J. (red.), *Kryminalistyka*, Warszawa 1999.

Wikariak, S., *Coraz więcej inwigilacji ze strony służb? Projektowane przepisy budzą kontrowersje*, "Gazeta Prawna online", 24 January 2023, https://www.gazeta prawna.pl/firma-i-prawo/artykuly/8644248,policja-sluzby-kontrola-operacyjna-inwigilacja-dostep-do-danych-komunikatory.html (accessed on: 04.06.2023).

Wójcik, E., *Czynności operacyjno-rozpoznawcze i ich rola w zwalczaniu przestępczości zorganizowanej*, https://wspia.eu/media/oojnsacq/44-w%C3%B3jcik.pdf (acessed on: 01.06.2023).