Humanities and Social Sciences **2024**
Research Journal 31, No. 2 (2024), pp 131-141 **April-June**

Received: March 2024
Accepted: June 2024
DOI: 10.7862/rz.2024.hss.24

Marta POMYKAŁA[1]

THE CENTRAL CYBERCRIME BUREAU AS A NEW POLICE SERVICE ESTABLISHED TO COMBAT CYBERCRIME

In 2022, a new police service, namely, the crime-fighting service, was created. The Central Cybercrime Bureau was also established as an organizational unit of the police, which is responsible for recognizing and combating crimes committed using IT systems, ICT systems, or ICT networks and preventing such crimes, as well as detecting and prosecuting their perpetrators. The aim of this paper is to assess the validity of separating the cyber police in the structure of the Polish Police and to analyze its place and role in the cyber security system. Subjects under consideration include the tasks and powers of the new service, problems related to the selection of qualified officers with specialized IT knowledge, and the problem of providing infrastructure enabling the effective implementation of the entrusted tasks. The research methods used in the paper are the dogmatic-legal method and the theoretical-legal method.

Keywords: cybersecurity, cyber police, The Central Cybercrime Bureau, operational and reconnaissance activities, service in the Police.

1. CYBERSECURITY AS AN ELEMENT OF MODERN STATE SECURITY

The intensive development of information technology, which has been taking place since the last decades of the 20th century, brings enormous changes in all spheres of life in modern society. Modern technologies influence business, and by providing completely new tools for managing operations and data analysis, streamline and facilitate commercial or manufacturing activities, they are the basis for quick communication between people located in different places around the world, enable wide access to information, and at the same time form the basis of modern education and entertainment. Today it would be difficult to find areas where such changes do not take place at all. All this has a huge impact on the life of modern man.

However, new technologies bring previously unknown threats and challenges to state security and the safety of individuals. Attacks against IT infrastructure, attacks using malware, data leaks and breaches of confidentiality, internet fraud, identity theft and cyber espionage are becoming an increasingly serious problem in today's society. Over recent years, the number of this type of threats has been systematically increasing and is related

[1] Marta Pomykała, Rzeszow University of Technology, Poland; e-mail: mpomykal@prz.edu.pl. ORCID: 0000-0002-2557-1876.

to the constant increase in the level of digitalization in modern society (Enisa threat landscape 2023, https://www.enisa.europa.eu...).

These phenomena quickly became known as cyber threats, and their specificity is noticed both in science and in practice. Cyber threat is a phenomenon in which a malicious attack occurs via the Internet or other information technologies on a single entity or organization (Lakomy, 2015; Wasilewski, 2023; Oleksiewicz 2017). This is a set of activities aimed at intercepting data, extorting money or passwords, as well as destroying information stored on the computer's hard drive. According to the current Cybersecurity Strategy of the Republic of Poland, a cybert hreat should be understood as any potential circumstances, event or action that may cause damage, disruption or otherwise adversely affect ICT networks and systems, users of such systems and other people (Resolution on the Cybersecurity Strategy...; Pomykała, 2021). In the light of this document, increasing the level of resistance to cyber threats and increasing the level of information protection in the public, military and private sectors and promoting knowledge and good practices enabling citizens to better protect their information is the main goal of ensuring state cybersecurity (Pomykała, Polinceusz, 2015).

In the modern world, where technology plays an increasingly important role, cybersecurity is systematically becoming one of the most important areas of state security. The concept of cybersecurity in a narrow sense only covers the protection of computer systems, networks and data against digital attacks, and is also included in the Act on the National Cybersecurity System of 2018 (Act on the National System...). In art. 2 point 4 of this Act, cybersecurity is defined as the resistance of information systems to activities that violate the confidentiality, integrity, availability and authenticity of processed data or related services offered by these systems. The Act implements Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of network and information systems within the territory of the Union (Directive on measures…).

Nowadays, when more and more aspects of our lives are moving to the digital space (commonly referred to as cyberspace), cybersecurity is no longer only a technical issue, but also a social and economic one. The digitization of all areas of modern life, universal access to the Internet, and unlimited range of communication networks facilitate various criminal activities, especially property, economic, drug and pedophile crimes. New technologies provide new tools for committing crimes, although they can also be targets of crime themselves (Kamuda, 2018). Without adequate protection in this area, both individuals and organizations may suffer serious financial and reputational losses. The understanding of cybersecurity is constantly evolving and expanding. It is undoubtedly a key element of state security and requires constant commitment and special attention from many entities (Żywucka-Kozłowska, Dziembowski, 2023).

Every modern state has institutions and services specialized in appropriate tools and means to combat security threats. However, combating cyber threats seems to be a completely new challenge, requiring additional skills, including good knowledge of the digital environment, specialized knowledge in IT and the ability to efficiently navigate in these areas. Today's cyber threats have long not constituted a uniform group of challenges, and specialized entities are created to combat them. Cybercrime, as a type of crime carried out using computer techniques and involving computer systems or networks, is a constantly growing and dangerous phenomenon. The perpetrators of cybercrime very often remain anonymous, the number of traces they leave, compared to traditional forms of crime, is negligible, which makes their detection very difficult. At the same time, it is worth

remembering that, given the global reach of cyberspace, cybercrime quite easily goes beyond traditional boundaries, and its effective combating increasingly requires extensive cooperation between law enforcement agencies of many countries.

2. ESTABLISHMENT OF A NEW POLICE SERVICE RESPONSIBLE FOR COMBATING CYBERCRIME

Combating crime has been the domain of the Police. Therefore, a natural consequence of the constantly increasing threat of cybercrime was the emergence of the idea of establishing a cyber police as a separate structure within the Police, prepared in technical, human and organizational terms to combat cyber threats, and at the same time focused on effective cooperation with similar entities in other countries. Since cybercrime is not, in principle, a separate type of crime, and its specificity is the emergence of new methods and means of committing crimes, the creation of a new entity responsible for cybersecurity protection was considered pointless (Justification for the government draft act..., https://www.europol...). Entrusting tasks related to identifying threats in cyberspace and combating cybercrime to the Police allows one to benefit from the previous experience of this formation in combating criminal crime and organized crime, as well as to maintain consistency in the scope of tasks performed, competences granted and the means and forms of action used.

Established in 2022, the Central Cybercrime Bureau (hereinafter: CCB) is an organizational unit of the Police used to combat cybercrime, which is responsible for recognizing and combating crimes committed using IT systems, ICT systems or ICT networks, and preventing such crimes, as well as for detecting and prosecuting their perpetrators. It also supports other organizational units of the Police in recognizing, preventing and combating specified crimes, as well as in detecting and prosecuting their perpetrators.

It should be emphasized, however, that this is not the first police unit established to combat cybercrime. Already in 2016, the Bureau was established within the structure of the Police Headquarters, which was entrusted with carrying out activities related to detecting perpetrators of crimes committed using modern ICT technologies. Appropriate organizational units were established at the provincial police headquarters and at the Metropolitan Police Headquarters and were subordinated to the relevant provincial police commanders (Capital Police Commander), who organized activities in this area within their resources. The Office for Combating Cybercrime acted as a coordinator of tasks carried out in training units. In practice, these units remained largely independent, and the implementation of tasks assigned by the Office was limited by the forces and resources available as well as locally set priorities (Michalecki, 2023). Such Police structures operated until the end of 2021, and the scope of their tasks regularly increased.

A special period was certainly the time of the Covid-19 pandemic, the first stage of which occurred in 2020–2021, when, due to the introduction of widespread isolation, greater social activity than before was concentrated online, significantly increasing the level of cybercrime threat (IOCTA Report 2020, https://www.europol.europa.eu/...). However, the detection rate of such events remains at the current, not very high level (Statistics for 2022, https://instytutcyber.pl...). Greater activity in cyberspace and the resulting greater number of adverse events were an important driver of organizational changes in the Police that took place at the beginning of 2022.

On January 12, 2022, the act establishing the CCB (Act on amending certain acts...) entered into force, as a result of which the management of the new unit was appointed in May 2022, and in July 2022 the first policemen started serving in it. First of all, the CCB received police officers who had transferred from the existing units for combating cybercrime at the Police Headquarters and provincial police headquarters. In the next stage, the recruitment of new officers began.

3. TASKS AND ORGANIZATION OF THE CENTRAL BUREAU FOR COMBATING CYBERCRIME

The Central Cybercrime Bureau is a specialized unit of the Police, which is an organizational unit of a new type of service, defined as the service for combating cybercrime (Act on the Police..., Article 4(1)(6), Article 5d(1)), whose task is to fight cybercrime throughout the country.

The organizational changes in the Police that were introduced with the establishment of the Bureau are an example of deconcentration of the administration that occurs in centralized administration, as a result of which a larger number of entities are separated at one administrative level and assigned to them to carry out specific types of matters. The most important goal of deconcentration is to make everything work better, faster and more efficiently (Niczyporuk, 2006). It is worth noting that over recent years, such organizational changes have been made several times in the Police, e.g. the separation of the Central Police Investigation Bureau, the Police Internal Affairs Bureau, the Central Police Forensic Laboratory, or the Central Bureau for Combating Cybercrime. These changes consisted in separating specific structures from the Police Headquarters and provincial headquarters and transforming them into organizational units that were auxiliary units of the newly created Police bodies. The effect of these processes was the dispersion of tasks and competences at one level, but maintaining the existing hierarchy in relations between Police authorities (Jaworski, 2023). As B. Jaworski emphasizes, such an organizational structure "better reflects the division of labor used in it, shows the connections between various functions and activities, highlights the degree of work specialization, and clearly presents the system of responsibilities" (Jaworski, 2023). The advantage of this solution is high specialization, which allows focusing on combating a specific group of threats. Equally important is the ability to concentrate resources in the form of specialized equipment and well-trained staff, which significantly contributes to increasing the effectiveness of tasks.

Pursuant to Art. 5d section 1 of the Police Act, The Bureau is responsible for the implementation of tasks throughout the country in the field of:

- recognizing and combating crimes committed using an IT system, ICT system or ICT network and preventing these crimes, as well as detecting and prosecuting the perpetrators of these crimes,
- supporting organizational units of the Police to the necessary extent in recognizing, preventing and combating these crimes.

Therefore, the tasks of The Bureau include preventing crimes committed using modern ICT technologies, recognizing and combating such crimes, but also supporting other Police units in conducting cases of this type. Therefore, The Bureau's interests include threats caused by ransomware attacks, DDoS attacks, malware, and threats resulting from defeating system security. The Bureaus has the power to take action in the face of crimes committed in cyberspace, and the group of these crimes has been systematically expanding

for several years. Currently, such criminal activities include: phishing, cyberstalking, spoofing, crimes on sales platforms, fake online stores, and fake payment gateways. The share of these crimes in the total number of crimes grows in proportion to the increasing degree of digitalization of society. Given the transnational nature of the Internet, it must be prepared to take action on both domestic and international issues. Therefore, an important task is also to combat crime against minors (sexual abuse, pedophilia) and to dismantle international criminal groups and detain their organizers as well as neutralize the technical infrastructure of these groups.

The management of the new Police unit was entrusted to the Commander of The Bureau. He is the direct superior of The Bureau police officers, and in the performance of his tasks he reports directly to the Chief Commander of the Police. The Commander is appointed from among Police officers and dismissed by the minister responsible for internal affairs at the request of the Commander-in-Chief of the Police, while the deputy Commanders of the CBZC are appointed from among Police officers and dismissed by the Commander-in-Chief of the Police at the request of the Commander of The Bureau. The seat of The Bureau Commander is the capital city of Warsaw (Police Act..., Article 5d, sections 2-5).

Following the example of the Central Police Investigation Bureau, an analogous organizational structure was introduced. The following organizational units have been established in The Bureau (Management regarding the temporary..., §6):

1) Special Board,
2) Criminal Intelligence Department,
3) Logistics Support Department,
4) General Department, Personnel and Training,
5) Department of Supervision and Coordination,
6) Division of Classified Information Protection,
7) International Police Cooperation Team,
8) Support Team,
9) Press Team,
10) Legal Team,
11) Psychological Support Team,
12) Control Team,
13) Occupational Health and Safety Team,
14) Boards and departments in all provincial cities.

The Commander of The Bureau has full personnel and training powers in relation to police officers of all organizational units of The Bureau (Police Act..., Article 5d(2)). This is a fundamental change compared to the previous situation, as before the establishment of The Bureau, the departments of the provincial and capital police headquarters were subordinated to the provincial commanders, and the directors of the Police HQ were not superiors of police officers in these units, so they could only coordinate their activities. Currently, after separating The Bureaus as a separate organizational division of the Police, it will be more effective to introduce uniform standards of case management throughout the country, coordinate proceedings, manage human and equipment resources, as well as set priorities in terms of categories of crimes that the office should investigate.

In order to carry out his tasks, the Commander of The Bureau is obliged to cooperate with other organizational units of the Police and relevant bodies and institutions, also from other countries (Police Act..., Article 5d(7)). Focus on broad international cooperation is a particularly important element in the work of The Bureau. Cybercrime knows no formal

borders and, like cyberspace, it is transnational. For the officers of The Bureau, the ability to maintain cooperation, training and exchange information with representatives of other countries, benefit from the experience of Europol and Interpol, as well as access to the latest software and technology will be of particular importance.

4. SERVICE IN THE CENTRAL CYBERCRIME BUREAU

The establishment of The Central Cybercrime Bureau is the first stage in the creation of the cyber police in Poland, and it will gain its full power only in the coming years. It only initiated the process of increasing police staff related to combating cybercrime. Ultimately, there are to be 1,800 of them. In 2025, each field unit (one in each voivodeship) should have at least 65 police posts, and the largest units – in Warsaw and Katowice – up to 140 posts (Justification for the government's bill..., https:// orka.sejm.gov.pl...). In the initial period in July 2022, 72% of the officers of the previous cyber department were transferred to the CBZC, and almost 80% of the ongoing cases were taken over. The remaining cases, due to their thematic scope, remained in the provincial headquarters (Sitek, 2022).

It was assumed that The Bureau would employ primarily people with knowledge and skills in the field of IT and modern ICT technologies. This resulted in a modification of the selection procedure for Police service by making it possible to profile the procedure towards candidates with specialized qualifications, education, authorizations or skills required due to the personnel needs of the Police. In the qualification procedure for a person applying for admission to CBZC, a very important stage was added in the form of checking knowledge and skills in the field of IT, the functioning of IT systems, ICT systems, ICT networks and knowledge of a foreign language in this area, and the possibility of extending the proceedings for conducting a psychophysiological examination (Police Act, Article 25(12)). At the same time, however, the obligation to conduct a knowledge test and a physical fitness test, as well as mandatory service adaptation in the Police prevention department or an independent Police prevention subunit, was waived.

New solutions are also provided for the remuneration of The Bureau officers. The existing rules for remunerating officers prosecuting cybercrimes did not seem particularly financially attractive for people with specialized IT education. For many years, there has been considerable competition in the IT industry, and the financial opportunities that can be achieved in the private sector are much greater than in public entities. Therefore, in recent years, the Police has also been struggling with the problem of outflow of qualified staff. The actions taken with the establishment of The Bureau were, therefore, aimed at reversing this tendency and encouraging IT specialists to take up service in the Police. Work in the Police related to combating cybercrime is to become financially attractive and bring earnings twice as high as in other Police services (New officers in The Bureau service, https://cyberdefence24.pl/...). Since the launch of recruitment for The Bureau, over 400 people have shown interest in the service, and 15 people have been accepted, however, the recruitment process is multi-stage and subsequent proceedings are still ongoing (Two years of The Bureau existence. There will be more positions, https://cyberdefence24.pl/...).

In art. 120b of the Police Act provides for the so-called ICT benefit, paid to police officers performing cybersecurity tasks. It is paid on the basis of the Act of December 2, 2021 on special rules for remunerating persons performing cybersecurity tasks (Act on special rules...). The decision on the payment of the benefit is issued by the police officer's

superior no later than 30 days after starting the performance of cybersecurity tasks, after conducting the official review process (Regulation on the amount of the ICT benefit...).

In art. 120c of the Police Act introduced an additional benefit related to serving in the CBZC. It is awarded to a police officer serving in a position related to the direct identification and combating of crimes committed using an IT system, ICT system or ICT network and the prevention of these crimes, as well as detecting and prosecuting the perpetrators of these crimes in The Bureau and to the policeman supervising these activities in The Bureau on a monthly basis. an amount not lower than 70% and not higher than 130% of the average remuneration of police officers. The amount of the benefit depends on the assessment of the fulfillment of duties and the implementation of the tasks and activities entrusted to the policeman. The decision on granting this benefit and its amount, for a period of one year, is issued by the Commander of The Bureau, and in the case of the Commander of The Bureau and his deputies – by the Chief Commander of the Police.

5. POWERS OF OFFICERS OF THE CENTRAL CYBERCRIME BUREAU

As already emphasized above, cybercrime is not a new type of crime, but it is carried out in a different space than previously known crime – in cyberspace. It uses completely new methods and means of operation, based on modern information technologies and computer networks. Therefore, all this requires an appropriate approach to recognizing the Internet environment, identifying new threats emerging there, and effectively responding to phenomena that are still at the forefront of prohibited acts (Pawelec, 2022).

When establishing The Central Cybercrime Bureau, no special powers of a different nature than those of the existing Police services already known from practice were provided for the new service. The powers of The Bureau are regulated by the same provisions that apply to the entire Police (Police Act, Articles 15–22), although when The Bureau was established, they were changed and extended to adapt them to law enforcement fighting crime in cyberspace. Today, The Bureau officers have the same powers as police officers of other units, so they can undertake operational and reconnaissance, investigation and administrative and order activities (Police Act..., Article 19).

Operational and reconnaissance activities are of key importance for combating crime. These are non-procedural technical and tactical activities developed by the practice of criminal law enforcement agencies, serving the preventive fight against crime (Taracha, 2006). It is worth noting that nowadays the scope of these activities is constantly expanding, especially in view of the need to combat increasingly sophisticated crime, such as organized crime or cybercrime, and the methods of prosecution require high activity and increasingly specialized knowledge of officers appointed to combat it and ongoing cooperation with the court or prosecutor's office (Momot, https://www.kryminalistika.org.pl...). The legal nature of operational and reconnaissance activities has long been considered ambiguous, due to the fact that they are not based on the provisions of the Code of Criminal Procedure (or the Code of Procedure in Petty Offenses), nor do they constitute administrative legal activities. This fact was emphasized for a long time by the lack of statutory regulation of this issue and the secrecy of lower-level legal acts regulating this activity. Currently, the legal basis for undertaking and carrying out operational and reconnaissance activities is specified in Chapter Three of the Police Act, which deals with the powers of the Police.

Operational and reconnaissance activities are classified activities that include information collection, data analysis, trace tracking, infiltration and other intelligence

techniques. They provide for the possibility of using provocation, a secretly supervised shipment or the purchase of a controlled purchase or a controlled bribe. Only state authorities that are granted such powers by law have the right to carry out operational and reconnaissance activities. However, private entities do not have them. Operational and reconnaissance activities are strictly regulated by law. When combating cybercrime, they may include in particular:

- monitoring websites, discussion forums, social networking sites and other platforms to detect irregularities, attempted attacks and suspicious activity,
- infiltrating criminal groups online in order to obtain information about criminal activities, the identity of perpetrators and planned attacks,
- searching computers, mobile phones and information media in order to identify perpetrators of crimes and prove their guilt, as well as reconstruct the course of events,
- tracking and analyzing digital traces (e.g. an analysis of digital data such as IP addresses, server logs, browsing histories) in order to gather evidence that can be used in a lawsuit.

In order to ensure appropriate effectiveness and efficiency of operational and reconnaissance activities carried out by The Bureau officers, in Art. 19 section 1 of the Police Act, the catalog of crimes in the case of which operational control may be used has been extended. It was supplemented with the crime of promoting pedophilia (Article 200b of the Penal Code), misleading public utility institutions as to the threat (Article 224a of the Penal Code), computer hacking (Article 267 § 1–4 of the Penal Code), (destruction of IT data (Article 268a § 1 and 2 of the Penal Code), computer sabotage (Article 269 of the Penal Code), disruption of network operation (Article 269a of the Penal Code), unlawful use of programs and data (Article 269b § 1 of the Penal Code), burglary – in the context of cash recorded in bank accounts (Article 279 § 1 of the Penal Code) and computer fraud (Article 287 § 1 of the Penal Code) (Kamuda, Trybus, 2023)

In art. 20 of the Police Act, changes were introduced to speed up obtaining information from entities providing payment services and enable more efficient tracking of funds derived from crime, by expanding the catalog of information and data that should be made available to the Police at the request of its authorized bodies and officers. In the past, refusal to provide such information often made it impossible to carry out further activities in a given case.

Additionally, it should be emphasized that the Commander of The Bureau has been granted powers similar to those previously held by the Commander of the Central Bureau of Investigation, related to operational control, controlled purchases, secret supervision of the production, movement, storage and trade of crime items, obtaining and using information constituting legally protected secrets and obtaining data that does not constitute the content of a telecommunications message, a postal item or a message as part of a service provided electronically. The Commander of The Bureau, therefore, became one of the Police bodies authorized to perform activities necessary to apply the above-mentioned measures and use the evidence obtained through them in further stages of proceedings against perpetrators of crimes.

6. CONCLUSIONS

The Central Cybercrime Bureau is a new and extremely necessary security protection service, which is becoming increasingly important for protection against cyber threats.

Cybercrime is not just a temporary trend, it is an inevitable consequence of technological development and the increasing use of modern information technology in all areas of modern life, including crime. The Bureau is also a response to the need for greater specialization of security services, and its creation allowed for the concentration in one place of forces and resources used to combat all forms of computer and internet crime, which should translate into increased effectiveness of activities in this area in the near future.

In order to effectively counteract all modern threats, security services must use the same means as criminals, and must also have personal and material resources to carry out their activities. Therefore, the fight against cybercrime requires appropriate adaptation of both organizational structures, but also tools and means of action. The establishment of The Bureau should, therefore, be considered an important, but only initial stage in this process. In the coming years, further challenges should be consistently addressed: ensuring sufficient staffing of The Bureau, providing its officers with access to the latest IT technologies, continuous training and professional development of officers, as well as the development of broad cooperation with similar entities from other countries and the widest possible exchange of information. Appropriate recruitment, as a result of which it is possible to select people with knowledge and experience in the field of IT, is a step in the right direction.

An equally important issue is the appropriate financing of The Bureau and its officers. Modern society can no longer afford to save on cybersecurity. The funds provided in the budget for the purchase of the necessary equipment and software are a necessary and indispensable condition for the effective and efficient implementation of its tasks. However, it is important that financing possibilities do not decrease when the office formation stage is completed. The creation of an incentive to take up service in The Bureau should also be assessed positively by providing additional funds for the remuneration of its specialists dealing with combating cybercrime, as well as the establishment of allowances for work in The Bureau, intended to encourage people with specialized education in IT to take up service.

REFERENCES

Jaworski, B. (2023). *Dekoncentracja rzeczowa w Policji – potrzeba chwili czy trend zmian? „Przegląd Policyjny”*, No. 2.

Kamuda, D. (2018). *Wybrane zagadnienia z zakresu cyberprzestępczości* [In:] Golonka, A., Trybus, M., ed., *Prawo karne w obliczu zmian i aktualnych problemów polityki kryminalnej*. Rzeszów: Wydawnictwo UR.

Kamuda, D., Trybus, M. (2023). *Cyber crime of reading info obstruction under art. 268 of penal code as a treat to security of the Republic of Poland. „Humanities and Social Sciences”*, No. 4/II.

Lakomy, M. (2015). *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*. Katowice: Wydawnictwo Uniwersytetu Śląskiego.

Michalecki, D. (2023). *Przestępstwa internetowe – zapobieganie i zwalczanie. „Kontrola Państwowa”*, No. 5.

Niczyporuk, J. (2006). *Dekoncentracja administracji publicznej*. Lublin: Wydawnictwo UMCS.

Oleksiewicz, I. (2017). *Rola służb specjalnych w polityce zwalczania cyberterroryzmu RP. „Humanities and Social Sciences”*, No. 3.

Pawelec, K. (2022). *Centralne Biuro Zwalczania Cyberprzestępczości i jego wybrane uprawnienia. Kilka refleksji. „Cybersecurity and Law”*, No. 1.

Pomykała, M. (2021). *Zapewnienie bezpieczeństwa wewnętrznego państwa jako zadanie administracji publicznej*. Rzeszów: Oficyna Wydawnicza PRz.

Pomykała, M., Polinceusz, M. (2015). *Problemy ochrony cyberbezpieczeństwa Rzeczypospolitej Polskiej w dokumentach strategicznych* [In:] *Współczesne zagrożenia cyberterrorystyczne i bioterrorystyczne a bezpieczeństwo narodowe Polski.* Warszawa-Dęblin: Wyższa Szkoła Policji w Szczytnie i in.

Sitek, E. (2022). *Cyberpolicja po nowemu. „Gazeta Policyjna”*, nr 12.

Taracha, A. (2006). *Czynności operacyjno-rozpoznawcze. Aspekty kryminalistyczne i prawnodowodowe.* Lublin: Wydawnictwo UMCS.

Wasilewski, J. (2023). *Zarys definicyjny cyberprzestrzeni. „Przegląd Bezpieczeństwa Wewnętrznego”*, No. 9.

Żywucka-Kozłowska, E., Dziembowski, R. (2023). *Wokół definicji cyberbezpieczeństwa. „Cybersecurity and Law”*, No. 2(10).

Dwa lata istnienia CBZC. Będzie więcej etatów [Access: 14.03.2024]. Access on the internet: https://cyberdefence24.pl/armia-i-sluzby/dwa-lata-istnienia-cbzc-bedzie-wiecej-etatow.

Enisa threat landscape 2023 [Access: 24.01.2024]. Access on the internet: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023/@@download/fullReport.

Nowi funkcjonariusze w służbie CBZC [Access: 11.03.2024]. Access on the internet: https://cyberdefence24.pl/armia-i-sluzby/nowi-funkcjonariusze-w-cbzc.

Momot, K. *Istota i zakres czynności operacyjno-rozpoznawczych* [Access: 11.03.2024]. Access on the internet: https://www.kryminalistyka.org.pl/artykuly/istota-i-zakres-czynnosci-operacyjno-rozpoznawczych/#_ftnref36.

Raport IOCTA 2020 (Internet Organised Crime Threat Assement) [Access: 10.02.2024]. Access on the internet: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf.

Statystyki za rok 2022 [Access: 10.02.2024]. Access on the internet: https://instytutcyber.pl/artykuly/statystyki-cyber-za-rok-2022/.

Uzasadnienie rządowego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości [Access: 11.03.2024]. Access on the internet: https://orka.sejm.gov.pl/Druki9ka.nsf/0/1DC336ABF6F97425C125878E003AC09A/%24File/1742-uzas.docx.

LEGAL ACTS

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

Act of April 6, 1990 on the Police (consolidated text: Journal of Laws of 2024, item 145).

Act of July 5, 2018 on the national cybersecurity system (consolidated text: Journal of Laws of 2023, item 913, as amended).

Act of December 2, 2021 on special rules for remunerating persons performing cybersecurity tasks (consolidated text: Journal of Laws of 2023, item 667).

Act of December 17, 2021 amending certain acts in connection with the establishment of the Central Bureau for Combating Cybercrime (Journal of Laws of 2021, item 2447, as amended).

Regulation of the Council of Ministers of January 19, 2022 on the amount of ICT benefits for persons performing cybersecurity tasks (Journal of Laws of 2022, item 131).

Resolution No. 125 of the Council of Ministers of October 22, 2019 on the Cybersecurity Strategy of the Republic of Poland for 2019–2024, (MP. of 2019, item 1037).

Order No. 1 of the Commander-in-Chief of the Police of January 12, 2022 on the temporary organizational regulations of the Central Bureau for Combating Cybercrime (Journal of Laws of the Police Headquarters of 2022, item 45).