The Role of the police in combating crime on the network

Marlena Lorek [*] [A]

***Corresponding author:** PhD in the field of security science, e-mail: mpotoczek@poczta.fm, ORCID: 0000-0002-6814-8162

[A] Rzeszów University of Technology, Warszawy, Poland

Received: March 1, 2023 | Revised: March 27, 2023 | Accepted: March 31, 2023

DOI: 10.5281/zenodo.7789813

Abstract

The police play one of the main roles in fighting crime online. In 2021, measures were taken to counteract computer crime. More than once, the Police have indicated criminals operating in the network, and this is why, from January 1, 2022, a cell responsible for fighting cybercriminals is to operate within it.

The purpose of this article is to show what forms of action are currently taken by the Police and which are to be introduced from 2022. The establishment of the Central Cybercrime Bureau is aimed at searching for criminals online, as well as catching pedophiles and those who want to steal their identity online. Such forms of crime are to be monitored and checked by officers who will work in the new Police unit.

The Polish system of combating crime, including cybercrime, meets the needs of those who have been affected by online crime. The need to create a new cell is also the aftermath of the scale of criminal events that took place in 2019 and 2020. Statistics at that time indicate that this problem is intensifying very much, because the current situation in the world has forced many of us to work or educate. The problem is growing every day, and criminals are looking for newer and newer forms of criminal activity.

The following considerations are intended to make you aware of the fact that online crime has many faces and it is worth paying attention to the websites you are using, as they may be fictitious in order to obtain all kinds of data. In addition, it is important to pay attention to what information users themselves upload to the network, as they may be used by criminals to intimidate or steal identity or image.

Key words: police, cybercrime, Central Cybercrime Bureau.

Introduction

Security is the most important element in the functioning of any society; therefore, states must properly assign tasks to uniformed services so that they can guarantee appropriate living conditions in a given territory. Efficient functioning of the state and individuals is possible only if the community is free to develop, work and educate (Lorek, M., 2017). Currently, not only the state is responsible for security, but also the citizens themselves, who develop their passions and tasks online. The Internet sets new trends in online threats that can be encountered every day, regardless of where we are in the world. Currently, the states, in consultation with uniformed services, but above all with the Police, should constantly conduct preventive activities in the field of education in the use of the Internet and threats that can be encountered in the virtual world. This forces the introduction of new forms of detecting and combating crime on the Internet, adequate to the threats.

Moreover, effective models for monitoring the effects of online crime should be created. The operators of individual websites constantly monitor threats and related crime (Misiuk, A., Kosiński, J., 2002), however, there are cases of interception of personal data (Kulesza J., 2010). Data theft and crime on the Internet is a fairly popular topic today, as the pandemic caused a large part of people's activity to move to the Internet. On the one hand, it was supposed to increase the personal security of citizens in the context of coronavirus threats, but on the other hand, the problem of computer crime in the virtual world is getting worse.

Results and Discussion

Police and their role in combating crime

The word "police" comes from the Greek "politeja", which meant city management. It took root in Latin as "politia". The police at that time had a fairly extensive scope of operation, as they dealt with all state functions, which included ensuring security and public order. The police are nothing more than a uniformed and armed formation, whose task is to serve the state in order to ensure an appropriate level of security. In addition, it deals with maintaining public order (Jurgilewicz M., 2017).

In Poland, the Police began to operate under this name on April 6, 1990 on the basis of the Police Act (Policja, 2005). The basic tasks of the Police are:

- protection of health and life against unlawful attacks that may lead to their violation;
- protection of safety and property in public transport and road traffic, as well as in generally accessible waters;
- cooperation with state, local government bodies and social organizations in order to protect against committing crimes and offenses of a criminogenic nature;
- detecting offenses and crimes and prosecuting their perpetrators;
- supervising municipal (city) guards and other formations, as indicated in separate regulations;
- control of order and administrative regulations that are required in public places;
- activities with other police forces outside Poland in order to detect crimes contained in separate regulations;
- processing, gathering and transfer of criminal information;
- maintaining databases that contain all information about the results and analyzes of DNA (Lorek M., 2017).

Moreover, the Police are part of the public administration and therefore are obliged to act in the public interest. In its activities, the police are based on laws and international agreements. The Police Act is not a single legal act which defines their tasks. Other acts are:

- security of mass events (The Act of 20 March 2009);
- protection of people and property (The Act of August 22, 1997);
- a state of natural disaster (The Act of 18 April 2002);
- state of emergency (The Act of June 21, 2002);
- road traffic law (The Act of June 20, 1997);
- foreigners (The Act of 12 December 2013).

The Internet has become an integral part of our everyday life, therefore, with the increase in the number of users, it has increased the range of using this knowledge carrier (The biggest threats). At the beginning of its existence, the Internet was supposed to increase access and provide opportunities to learn about the world using mobile devices (Jedlińska R., 2017). Unfortunately, over time, criminals also moved online. It is worth adding that many internet users are unaware of the online dangers and how easy it is to become a victim of cybercrime. Fraud is the largest group of internet crimes (Marek A., 2007).

The police work to search for perpetrators of crimes online. Currently, the Department for combating cybercrime operates within its structure. This unit deals with counteracting such forms of crime. The Internet offers many opportunities to commit a wide range of crimes, and their scale is unlimited (Police). The police act in the field of inappropriate activity of Internet users so that they cannot violate someone else's property, independence or freedom of action with impunity. The worst part of all this is that the Police do not have the appropriate means by which they can quickly punish a person who has committed a prohibited act online. It is possible only after amending the law on crimes committed online, because a crime in this area is very difficult to prove to the perpetrator. Internet crime has been penalized only partially in the Polish Penal Code of 1997 (Cybercrime Department).

The scale of online crime is large and is growing every year, so it is worth taking steps to

include online crimes in one of the chapters of the Penal Code. Failure to do so causes problems when it comes to punishing the perpetrator. At the same time, it must be borne in mind that such a solution is temporary, because the turbulent situation regarding the rapid appearance of new types of crimes on the Internet will force constant adaptation of the law (What's happening on the web). Along with the development of the network and the creation of new programs and applications, the scale of this phenomenon will grow dynamically, and proper protection of internet users is not possible, because the Police are not technologically prepared, so online criminals have an advantage.

Characteristics of crime

Crime is defined as all the acts prohibited by law. The consequence of their committing is a criminal sanction. These are activities that took place at a specific time and within a specific territorial unit. A prohibited act is behavior contrary to applicable law or accepted standards. On the other hand, within the meaning of the Criminal Code, it must be an act prohibited under penalty of a binding act defining its features (Coronavirus and economic crime).

B. Hołyst indicates that crime is nothing else than the general offenses prohibited by law in a given area, and their violation may lead to criminal sanctions (Hołyst B., 2016). Currently, crime is one of the main social problems. In recent years, internet crime has come to the fore. It negatively affects the economy of a given country. Even though it is not so easy, many countries have set themselves the goal of fighting online crime (Dylematy cywilizacji informatycznej, 2004). Individual countries allocate a lot of resources and effort to fight this phenomenon (Wierzbicka A., 2015), which may lead to the loss of personal data, image, property or money (Błachut J., 2007). On the Internet, we often deal with organized crime groups (Wójcik J.W., 2001). Many criminal activities are not reported at all because they are so-called low harmfulness, therefore the perpetrators act in such a way as to avoid the consequences of being washed as much as possible (Mordwa S., 2013). Often, the perpetrators of crimes have adequate knowledge and means to act to avoid criminal liability (Szczechla E., 2017). Technological development generates newer and newer forms of activity, but also the fact that younger and younger people commit criminal acts online, because they do not have adequate knowledge, what is good and what is bad, and how easy it is to cross the barrier that can lead to legal consequences. The Internet allows for efficient operation and speed in earning money from various forms of crime, which prompts young people who want to exist and earn money quickly for such criminal acts (Karpiel D., 2017).

Cybercrime department

The cybercrime unit in the police is currently countering a wide range of different types of crime (Kosiński J., 2015). The methods of online crime perpetrators are described below:

1. Hacking attacks: it is hacking access to e-mail boxes, computer programs of large companies, often by impersonating a given institution in order to reach their customers and intercept their personal data or funds (Cieśla W., 2021).
2. Malware: This is an attack on customers who use online banking. Such activities include the Banatrix Trojan, which is designed to search the memory of web browsers in order to obtain a sequence of numbers that correspond to the bank account number, which allows you to change it at a given moment and redirect funds to another account indicated by criminals (Siwicki M., 2013).
3. Botnet: is a group of computers that has been infected with a virus that allows criminals to remotely control these devices. The perpetrator can block websites through DDos attacks in order to obtain funds for restoring the functioning of a given network (What is a botnet?).
4. Identity theft and money laundering: This criminal act is most often done by sending attractive job offers to users. The offered work is on preferential terms and with a significant remuneration (Identity theft). The criminal wants to obtain sensitive data from the person found ("Smishing", a scam using SMS).
5. False bids to buy and sell: These scams are best carried out with a buy or sell offer. The scammers' offers are very attractive (How to safely buy online?). Finally, interested in the offer, pays money quickly, but does not receive the purchased goods.
6. Nigerian Fraud: This is done via email. Fraudsters often ask for financial help, and in

return for the funds received, they offer a part of the amount that will come, for example, from their inheritance (Nigerian scam).

7. SMS fraud: the perpetrator encourages the user to visit various types of websites, for example those that test our intelligence. After solving such tests (Office of Electronic Communications) the user who wants to check the result can receive it via SMS, however, he must meet certain conditions for sending the message. First, send a paid message, the price of which is not specified, and after making the payment, it turns out that the perpetrator has extorted a much larger amount of money (VOICE PHISHING).

8. Ransomware blackmail: the first crimes of this type consisted in blocking users' computers and pointing out that the perpetrators of such action were law enforcement agencies (Gigabyte ransomware attack). Currently, fraudsters use measures to encrypt data and victims are then unable to use their disks and important documents (What is ransomware?).

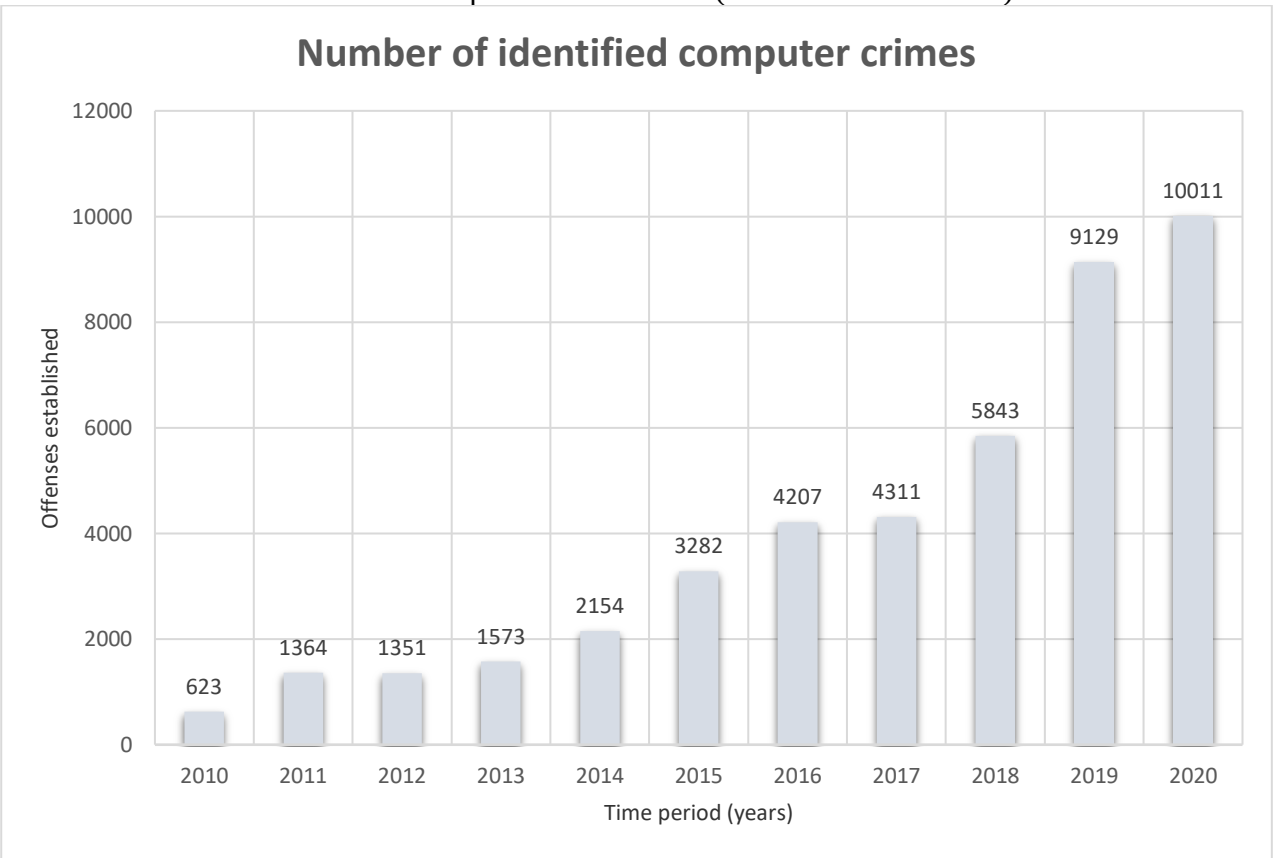

Figure 1 – Number of identified computer crimes
Source: own study based on: www.policja.pl (15.11.2021).

As can be seen in Figure 1, the dynamics of crimes since 2010 is quite high, because from year to year it can be seen that the Police record more and more incidents of this type online. The last two years stand out against the background of the analyzed decade – the time of the pandemic. The tendency to use the Internet increased then, as the activity in the real world was reduced to the necessary minimum. This has given criminals more opportunities to commit such computer crime related acts.

New forms of counteracting computer crime to be introduced in the Police in 2022

The threats appearing in the network mobilized the authorities to take action to combat this type of crime. The pandemic has shown how many challenges there are in this space. Public administration bodies and the Police are looking for new solutions in the field of counteracting crimes in cyberspace. Therefore, in Poland, it was decided to establish a new organizational unit within the Police structure, the activities of which will focus on combating cybercrimes (Hackers in telework).

On July 27, 2021, at a conference at the Chancellery of the Prime Minister, it was announced

that the Central Cybercrime Bureau would be established. The police will already have the appropriate instruments to act to combat online crime. Thus, it will operate more efficiently in this regard (The Central Office). The most important tasks of the Central Cybercrime Bureau will include:

- combating fraud related crimes;
- fight against online identity theft;
- fighting pedophiles who search for victims online.

This office will also be responsible for combating crime committed with the use of an IT system, an ICT system or an ICT network. Such activities will be aimed at easier detection of perpetrators and supporting other organizational units of the Police in recognizing, preventing or combating crime in cyberspace. The Commander of the Central Crime Combating Bureau will report to the Commander-in-Chief of the Police. The activities to be performed by the Bureau will result from the Police Act. The Central Cybercrime Bureau will be located in Warsaw. It will conduct activities in the field of:

- operational and reconnaissance;
- investigative;
- administrative and orderly.

A different qualification process will be applied to the officer of the new unit, as IT skills and knowledge of new technologies, as well as knowledge of a foreign language, will mainly count. A new recruitment path will be applied to these officers as they will be exempt from fitness tests. The police need IT specialists, therefore future employees will receive a fixed salary in the amount of 70–130% of the average salary in the Police. The creation of a new unit within the Police structure may turn out to be a major breakthrough in the fight against online crimes (The Polish government).

Conclusions

Currently, we are dealing with new types of crime, including cybercrime. The Internet has dominated the world and introduced new trends in the activities of criminals. The reduction of the fear of crime is related to the state's criminal policy towards the perpetrators of criminal acts. It is primarily about the quality of the law, which is a guarantee that every criminal act will be properly punished. But even the best law will be worthless if there is no inevitability of the punishment it envisages. Therefore, states should take preventive and educational measures in relation to network users and strengthen institutions responsible for ensuring the safety of citizens.

Responsibility for reducing crime lies not only with law enforcement agencies, but also with the society, which should react to adverse effects, which in turn may reduce crime, detect it and have a positive impact on the economy (Ziomka Z., 2008).

References

Błachut J., *Problemy związane z pomiarem przestępczości* (*Problems related to the measurement of crime)*, Wydawnictwo Wolters Kluwer, Warszawa 2007.

Cieśla W., *Bezpieczeństwo w cyberprzestrzeni (Security in cyberspace)* [w:] *Bezpieczeństwo państwa i jednostki – analiza wieloaspektowa (State and individual security – multifaceted analysis)*, red. M. Lorek, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2021.

Coronavirus and economic crime. Available from : https://codozasady.pl/p/koronawirus-a-przestepczosc-gospodarcza (6.05.2021).

Cybercrime Department. Available from : https://docplayer.pl/31687548-Wydzial-do-walki-z-cyberprzestepczoscia.html

Dylematy cywilizacji informatycznej (Dilemmas of information civilization), red. A. Szewczyk, Polskie Wydawnictwo Ekonomiczne, Warszawa 2004.

Gigabyte ransomware attack. Will the company bend under the blackmail of cybercriminals? Available from : https://ithardware.pl/aktualnosci/gigabyte_ofiara_ataku_ransomware_firma_ugnie_sie_pod_szantazem_cyberprzestepcow-17339.html

Hackers in telework. They are not complaining about COVID-19. Available from : https://www.forbes.pl/technologie/hakerzy-w-pandemii-koronawirusa-liczba-cyberatakow-szybko-rosnie/nqztk7s

Hołyst B., *Kryminologia (Kryminologia)*, Wolters Kluwer, Warszawa 2016.

How to safely buy online? 7 steps to detect a fake online store. Available from : https://kwestiabezpieczenstwa.pl/zakupy-online/

Identity theft. Available from : http://www.oszustwsieci.pl/kradziez_tozsamosci.php

Jedlińska R., *Problem przestępczości elektronicznej (The problem of electronic crime)*, "Ekonomiczne Problemy Usług" 2017, № 1(126), t. 2.

Jurgilewicz M., *Rola podmiotów uprawnionych do użycia lub wykorzystania środków przymusu bezpośredniego i broni palnej w ochronie bezpieczeństwa i porządku publicznego (The role of entities authorized to use or use means of direct coercion and firearms in the protection of public safety and order)*, Wydawnictwo Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2017.

Karpiel D., *Przestępczość zorganizowana (Organized crime)*, „Internetowy Przegląd Prawniczy TBSP UJ" 2017, nr 7.

Kosiński J., *Paradygmaty cyberprzestępczości (Cybercrime paradigms)*, Difin, Warszawa 2015.

Kulesza J., *Międzynarodowe Prawo Internetu (International Internet Law)*, Ars boni et aequi, Poznań 2010.

Lorek M., *Motywowanie w polskiej policji (Motivating in the Polish police)*, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2017.

Marek A., *Kodeks karny. Komentarz (The Penal Code. Comment)*, Warszawa 2007.

Misiuk A., Kosiński J., *Przestępczość teleinformatyczna (ITC crime)*, Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2002.

Mordwa S., *Przestępczość i poczucie bezpieczeństwa w przestrzeni miasta – przykład Łodzi (Crime and a sense of security in the city space - an example Łodzi)*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2013.

Nigerian scam – how to recognize it? Available from : https://blik.com/oszustwo-nigeryjskie-jak-je-rozpoznac

Office of Electronic Communications. Available from : https://www.uke.gov.pl/blog/strzez-sie-smishingu,21.html

Police. Available from: www.policja.pl

Policja w strukturach administracji publiczne (Police in the structures of public administration), red. A. Babiński, P. Bogdalski, Szczytno 2005.

Siwicki M., *Cyberprzestępczość (Cybercrime)*, C.H. Beck, Warszawa 2013.

Smishing", a scam using SMS. Available from : https://www.infor.pl/prawo/prawa-konsumenta/konsument-w-sieci/5256121,Smishing-czyli-oszustwo-wykorzystujace-SMS.html

Szczechla E., *Wizualizacja danych wielowymiarowych i danych geograficznych w procesie prognozowania przestępczości (Visualization of multidimensional and geographic data in the crime forecasting proces)* [w:] *Prognozowanie kryminologiczne w wymiarze społecznym (Criminological forecasting in the social dimension)*, red. B. Hołyst, Wydawnictwo Naukowe PWN, Warszawa 2017.

The Act of 12 December 2013 on foreigners (Journal of Laws of 2013, item 1650).

The Act of 18 April 2002 on the state of natural disaster (Journal of Laws 2002, No. 62, item 558).

The Act of 20 March 2009 on the safety of mass events (Journal of Laws of 2009, No. 62, item 504).

The Act of August 22, 1997 on the protection of persons and property (Journal of Laws 1997, No. 114, item 740).

The Act of June 20, 1997 – Road Traffic Law (Journal of Laws 1997, No. 98, item 602).

The Act of June 21, 2002 on the state of emergency (Journal of Laws of 2002, No. 113, item 985).

The biggest threats on the Internet in 2021 – how to recognize them and how to fight them? Available

from : https://scroll.morele.net/poradniki/najwieksze-zagrozenia-w-internecie-w-2021-jak-je-rozpoznac-i-jak-z-nimi-walczyc/

The Central Office for Combating Cybercrime is being created – almost 2,000 officers will handle cases. Available from : https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/powstaje-centralne-biuro-zwalczania-cyberprzestepczosci-sprawami-zajmie-sie-prawie-2/mp8189n

The Polish government is setting up a unit to fight hackers - that's good... but we have some concerns. Available from : https://www.benchmark.pl/aktualnosci/powstaje-centralne-biuro-zwalczania-cyberprzestepczosci-znamy.html

VOICE PHISHING or fraud using a telephone connection. Available from : https://www.bskazimierzdolny.pl/voice-phishing-czyli-oszustwo-z-wykorzystaniem-polaczenia-telefonicznego.html

What is a botnet? Available from : https://www.politykabezpieczenstwa.pl/pl/a/czym-jest-botnet

What is ransomware? Available from : https://www.trendmicro.com/pl_pl/what-is/ransomware.html

What's happening on the web. Available from : https://gazeta.policja.pl/997/rchiwum-1/2018/numer-154-012018-1/154910,Co-sie-czai-w-sieci.html

Wierzbicka A., Żółtaszek A., *Analiza bezpieczeństwa publicznego w krajach europejskich (Analysis of public safety in European countries)*, "Wiadomości Statystyczne" 2015, nr 8.

Wójcik J.W., *Przeciwdziałanie przestępczości zorganizowanej. Zagadnienia prawne, kryminologiczne i kryminalistyczne (Organized crime prevention. Legal, criminological and forensic issues)*, Wolters Kluwer, Warszawa 2001.

Ziomka Z., *Przyczyny zachowań przestępczych oraz zjawisk patologicznych w świetle teorii socjologicznych (The causes of criminal behavior and pathological phenomena in the light of sociological theories)*, Wydawnictwo Szkoły Policji w Katowicach, Katowice 2008.