DOI: 10.5604/01.3001.0013.1759 ASEJ ISSN: 2543-9103 ISSN: 2543-411X (online)

Contemporary threats related to content processing in the cyberspace

Kamil Martyniak [1], Dariusz Szydłowski [2]

[1] Bielsko-Biała Police Headquarters
ul. Wapienna 45, Bielsko-Biała - Poland

[2] Department of Law and Social Sciences, Bielsko-Biała School of Finance and Law
ul. Tańskiego 5, Bielsko-Biała - Poland

***Abstract*— The Internet, as a social medium has a wide spectrum of applications. In general, the cyberspace serves as a provider of services, a commercial platform and the arena of social networking. On one hand, the Internet offers unlimited possibilities with respect to the access to all sources of information but, on the other hand, it can generate a series of threats to the established social and legal order. The threats may pertain to systems, data security, computer programs, users' privacy and intellectual property. Although the problem is important socially as well as politically, until recently the Polish literature on the subject did not address the issue of counteracting and punishing offences related to electronic data processing widely enough. The motivation behind this paper was recent social discourse on the free flow of information on the Internet and the multiplicity of controversies accompanying this topic.**

Index Terms— cyberspace, the law, the Internet, computer crimes, information, cybersecurity

I. INTRODUCTION

Poland adapted its legal system to the reality of the so-called information revolution in 1998. The scope of criminalization of abuses related to the use of information technologies for the dissemination of illegal and harmful content and the rules of liability of entities involved in the dissemination of information prohibited by law, is determined by the Act of 6 June 1997 Criminal Code and the Act of 18 July 2002 on the provision of electronic services. The aim of the act was to standardize the area not yet regulated in the Polish legal system and to adjust the adopted solutions to the Community Law (Adamski, 2000). In the literature on the subject authors have not yet agreed on a uniform term which could be used to define the group of prohibited acts related to the use of computer systems and ICT networks to disseminate information prohibited by law. When describing the essence of such crimes, the following terms are used: 'crimes related to digital technology', 'crimes related to the technology of information processing' or 'internet crimes' (Adamski 2000). Other terms include 'computer crime' or 'crime using advanced technologies' (Communication from the Commission to the European Parliament, the Council and the Committee of the Regions 2007). At the same time, this kind of crime is often classified as cybercrime or computer crime in general (the group of acts known as cybercrime involves the use of information systems or networks to violate any legal interest protected by criminal law). Cybercrime also includes attacks on systems, data and software, a group of acts commonly referred to as computer crimes or crimes against the security of processed information.

II. ATTEMPTS TO PUT BOUNDARIES ON THE CYBERSPACE

When discussing the issue of jurisdiction and law applicable to the Internet, it is necessary to mention the idea propagating creation of an autonomous branch of law for the cyberspace which since the beginning of the existence of the global open computer network has won many advocates (Johnson, 1996). Some authors consider it legitimate to undertake efforts to regulate the Internet as a separate domain (a reality different than the material world) with its own legal order (Post, 2009). Such a separate legal order would refer to torts related in particular to such areas as: copyright, industrial property rights, protection of personal rights or selected issues of press and civil law (Barta, 1997). Establishing a separate cyberspace legal system, according to the proponents of this concept, would eliminate doubts related to jurisdiction and applicable law. What is more, it would enable development of new legal structures specific only to the Internet without the risk of violating the existing legal paradigms e.g. in the sphere of copyright (Barta, 1997). This law could also deal with the issues of the flow of protected goods (e.g. works) between the real world and the computer network.

The concept of a legal system specially dedicated to the cyberspace has been criticized by some authors (Kronke, 1998) who observed that there is no such thing as cyberspace within the meaning of a separate space that would be regulated by

ASEJ - Scientific Journal of Bielsko-Biala School of Finance and Law
Volume 23, No 1 (2019), pages 5
DOI: 10.5604/01.3001.0013.1759
Received: 18 December 2018; Accepted: 11 March 2019

Regular research paper: Published: 30 April 2019
Corresponding author's e-mail: szydlowski@autograf.pl; kamil.m.martyniak@gmail.com

separate international private law. Unlawful acts are always committed in a specific real and traceable area, damage occurs in the real world, usually within the strict territorial framework of a given state. However, determination of the location of the crime scene or evaluation of effects of the crime, is a completely different matter. Moreover, it does not prejudge the need to exclude the application of the current conflict-of-law- rules, justifying it with some unspecified virtual space. On the contrary, it is still justified to look for jurisdiction of the courts and the relevant acts in force in the states concerned, although it must be admitted that, as a rule, there will be a great number of courts and country specific laws involved. H. Kronke emphasizes that having read the literature on cyberspace which deals with both hypothetical and actual court cases, he has never encountered cases in which the deeds or their effects could not be linked to a real space and a corresponding legal order (Kronke, 1998). H. Kronke does not deny, however, that the Internet is characterized by many specific features that call for modification of existing regulations. The features include: significant difficulties in identifying the websites, a decentralized way of sending information, the jurisdiction of courts or laws of countries through which information or its part flows (which is a characteristics of a network), or which contain certain technical means, such as servers, possibility of access to information by unauthorized persons (e.g. server administrators), the existence of systems of links between websites, and most importantly, potentially widespread availability of all types of tort information (Świerczyński, 2004).

According to K. Węderska, there are four main areas related to the cyberspace: law, space, security and threats. Each of the areas is connected with a number of specific problems such as incoherence and lack of international standards in the area of law, lack of spatial, geographical boundaries or the lack of uniform solutions regarding the security of virtual networks (Table 1).

TABLE 1.
AREAS OF SPECIFIC CYBERSPACE RESTRICTIONS

Area	Characteristic
LAW	• unclear law or inconsistent law; • unclear responsibility for acts and offences; • lack of international (national) classification and qualification criteria; • imprecise determination of criminal acts and acts of national security threats.
SPACE	• lack of spatial boundaries; • lack of political boundaries; • lack of geographical boundaries; • lack of ad-hoc borders.
THREATS	• simple, generally available technology; • anonymity of the case; • many forms of cyberattacks; • 'domino effect'; • features of 'weapons of mass disorganization'; • low cost of attacks.
SECURITY	• lack of fast and effective security solutions; • a multitude of threat objects (attacks); • high security costs; • varied susceptibility of objects; • unpredictability of threat sources; • very high costs.

Source: (Sienkiewicz, 2015).

The question of the jurisdiction of the state with regard to virtual space is of particular importance for criminal proceedings. The system of justice and law enforcement agencies in particular, can be confronted with considerable problems when acts prohibited by law of a given country are carried out by a person or through a server located in another country. Similarly, in the case of typical computer crimes, such as hacking, computer sabotage or cyberterrorism, it turns out to be problematic to determine location of the crime scene as the cybercriminal may be located in another country and may use a wireless Internet or telephone connection which makes him difficult to locate. The number of such incidents is growing in Poland which poses a real challenge for the system of justice and for law enforcement agencies. More and more often, the Police officers and law practitioners are forced to cooperate with specialists in the field of information technology.

III. THREATS

The existence of the information society is generally a positive phenomenon, however with time one can observe the emergence of previously unknown dangers and threats. The phenomena and processes occurring in the cyberspace go far beyond the technical dimension, taking on a social character. *We are currently witnessing the formation of the so-called information society, that is, regardless of various attempts, impossible to define, a society with profound changes in social awareness caused by the digital revolution which has multidimensional, economic, political, cultural and social impact on the surrounding reality by means of information. This society is sometimes referred to as a society of risk, due to the possible implications of threats to the security of individuals and human communities* (Białoskórski, 2011). Threats in the cyberspace affect individuals, social groups, organizations and entire nations.

Each of the existing IT and telecommunication systems may be associated with specific threats and susceptibility to certain criminal activities. The first group of threats is sabotage and unintentional acts causing damage but without direct material or informational gain for the perpetrator. This category includes power supply failures, fires, natural disasters, disintegration as well as other physical destructive factors. Computer viruses, logical bombs and Trojan horses can be a form of disintegration or computer destruction and physical destructive factors include explosive devices that destroy computer equipment (Czechowski, 1993). The second group of threats is created by infiltration, i.e. actions of unauthorized persons aimed at penetrating various elements of the IT system or telecommunications network in order to obtain information by various means and in many different ways (Czechowski, 1993). A characteristic feature of this method is the intention of the criminal to obtain profit from the acquired information. Infiltration is divided into two categories - active and passive.

Passive infiltration is tracking information at a specific place in its circulation using the following techniques:

- electromagnetic interception consisting either of access to the connections between a computer and terminals, or in directional emission of radiation and on the analysis of the reflected signal by a radiating device;
- joining a data transmission line in telecommunication networks or intercepting radio signals;
- researching and copying unsecured resources (computer piracy);
- analysis of waste paper or residue from information carriers, resulting from either carelessness in the waste paper policy or disregarding the obligation to demagnetize information carriers;
- use of concealed transmitters (Czechowski, 1993).
- Active infiltration is the conscious acquisition of access to the system in order to interfere in the most sensitive and most important links. Active infiltration often takes the following forms:
- breaking security features in order to access any place in the IT system while bypassing the security devices used by the legal system user (for example getting through to the security registry);
- interference in the structure of operating systems;
- impersonating an authorized user of the computer system;
- application of additional programs and procedures (either during the software development phase or exploitation phase) (Czechowski, 1993).

The information war may take many forms. P. Sienkiewicz and H. Świeboda indicate four methods of attack: electromagnetic, fire, psychological and misinformation. Each category will trigger further effects of direct nature (Table 2). The goal, however, is always the same: weakening the opponent, disinformation and destruction of resources.

TABLE 2.
AN EXAMPLE SCENARIO OF THREATS ON THE COUNTRY LEVEL

Type of destructive acts	Direct effect	Further effect	Counteraction
Electromagnetic attack`			
The release of electromagnetic impulses in the areas of the network nodes. Launch of devices interfering with the wireless communication transmitters.	Disinformation. Transmission of false information by e-mail and other means of social communication.	Loss of administrative information. Disruption of work or paralysis of the city administration system. Increased sense of threat and social discontent.	Detection and assessment of threats. Resistance of equipment and rooms to electromagnetic attack. Organizing the system recovery after the attack.
Fire attack			
Detonation of explosives within network nodes. Interruption of network lines.	Destruction of telephone exchanges and server rooms –paralysis of network operation. Disruption of work or paralysis of the city administration system.	Loss of administrative information. Disruption of the state administration system. Increased sense of threat and social dissatisfaction.	Detection and assessment of threats. Physical resistance of the network to a fire attack. Organizing the system to restore its efficiency after the attack.
Psychological actions			
Social engineering – attracting the office staff to participate in the attacks.	Enabling access to the IT network of state administration systems, disclosure of classified information. Internal sabotage by the recruited staff. Financial fraud made by administration employees.	An external IT attack on the network. Threat to information security of the state. Theft of classified information (e.g. personal or financial data). Deterioration of financial security. Disturbances in the administration of the state. Increased sense of threat and social dissatisfaction.	Detection and assessment of threats. Raising awareness of personal conditions. Improvement of the procedures for controlling access to information.
Disinformation			
Sending false information by e-mail and other means of social communication.	Questioning the honest intentions of the authorities and management of the organization of the state administration system. Challenging the credibility and qualifications of selected groups of staff. Disseminating false information about the intentions of the state authorities. Providing false information about work for the benefit of the interests of foreign countries and organizations by representatives of the authorities.	Rising concern, worsening moods, attempts to spread panic, worsening the quality of the state's functioning. Attempts to undermine the financial stability and liquidity of the state. Increased sense of threat and social dissatisfaction.	Quick reaction of the authorities to false information. Efficiently reaching out to population and staff of companies with objective information. Keeping the truth in information. Detection and stigmatization of dis-informers.

Source**:** (Sienkiewicz, Świeboda, 2004).

The state may be exposed to various kinds of threats aimed at weakening the center of power. The threats may include: physical attacks on systems and networks causing destruction of electronic devices and electrical data communication networks, telephone exchanges or disruption or paralysis of these networks. The information war also takes place in the mental zone through chaos, disinformation of the society and the use of social engineering to persuade state personnel to participate in the attacks. The information war may be carried out both by state entities e.g. armed forces but also by non-state entities which may affect the security of the state. If the perpetrators come from within the centre of power the threats they create are systemic (state organizations, terrorist organizations or organized criminal groups). If the perpetrators are non-state entities they generate the so called common threats posed by vandals, hackers and crackers. Operations of non-state perpetrators usually proceed in three stages. First, the weaknesses of the system or object are recognized, then the access to the system or object is gained, whereas the final stage may take the form of theft, data copying or modification (Sienkiewicz, 2006).

In theory, the most serious consequences may be triggered by a cyberattack conducted by one state on another. Such a form of aggression could be considered as an attack within the meaning of Article 5 of the North Atlantic Treaty (North Atlantic Treaty, 1949) and could consequently lead to international conflict and armed intervention. In practice, however, the organizers of cyberattacks usually belong to the group of non-state entities. There are several reasons for this. Firstly, in case of state services, the decision must be formalized, subjected to plans, procedures and official subordination. In decentralized structures, however, it is possible to take appropriate steps following a unilateral decision taken by the leader or a narrow group of people. In case of an attack carried out by a single person, the decision may be made on the spur of the moment dictated by current emotional state of the perpetrator. Secondly, in case of non-state attackers, an electronic action is often the only way to achieve their goals. When it comes to state entities, the range of possibilities is much wider. Law theorists claim that states have many instruments to influence foreign governments and therefore use electronic attacks with considerable caution as they fear serious consequences on the international arena (Trelikowski, 2009).

IV. COUNTERACTING CYBER ATTACKS

Statistics suggest that sooner or later each company will suffer as a result of a cyber burglary or a system breakdown caused by a serious breach of security. Therefore, it is impossible to fully secure the company. What companies can do is to postpone this moment in time and consciously minimize the losses caused by the incident. This can be achieved primarily through the preparation and implementation of emergency and anti-burglary plans. This can be done by building up an internal security department or by using specialized IT suppliers. The security system should include simple automatic backup services as well as complex outsourced security with a turnkey 'backup' data center. The IT market also offers solutions that protect applications, websites or online stores from the effects of DDoS attack causing server paralysis.

Effective protection against security breaches is always a consequence of certain compromises. Therefore, when working on a security system, first question the management needs to answer is which elements of the IT infrastructure are the most important. At the same time, it is worthwhile to set the priorities with respect to the field of IT security. According to specialists in data protection, the list of basic threats includes issues related to the use of mobile devices (45%), uncontrolled use of social media (32%), processing in the cloud (cloud computing) and unaware or negligent actions of employees (computerworld.pl, 2019). Preventing network attacks is a priority in any security system. However, once such an attack occurs, it is essential to have a transparent process for detecting threats and applying countermeasures. Once an intrusion has been detected, users, devices and content should be quarantined using automatic and manual systems in order to protect the company's network and data resources. Information on previously unknown threats should be forwarded to relevant points and thoroughly analyzed. As a result, updates will have to be sent back to various services on the network and each layer will receive the right combination of current security features.

There is no single technology for effective protection against attacks. The key to success is the proper integration and interoperability of many systems. Each component plays a different role and cooperates with others. It is expected that cybercriminals will implement new developments and will focus even more attention on misleading users and bypassing security. Golden mean does not exist, but a multi-layered solution based on tested methods and state-of-the-art technologies will break the chain of advanced attacks with long-lasting effects (Downloads/how-to-protect-before-cyberattacks-about-long-term-action,2019/Downloads/jak-sie-bronic-przed-cyberatakami-o-lugotrwalym-dzialaniu, 2019).

The measures taken to prevent cybercrime cannot be limited only to the adoption of appropriate legal regulation as these are not able to stop all cases of illegal Internet use (Siwicki, 2011). Due to the complexity of the phenomenon, the implementation of criminal law for cyber offences is still a novelty for criminology and for the legal system as it requires a deep insight into the technical area of data processing systems (Wójcik, 2011). Offenders often benefit from differences in the scope of criminalization or technological solutions that makes them very difficult to identify. Therefore, the most effective weapon against criminal behavior is minimization of risk through selection of appropriate Internet service providers and raising awareness of users. Such approach will bring better results than repressive criminal punishment (Siwicki, 2011). Perfection of methods and application of technical procedures aimed at protection of the legal interest i.e. an electronically processed piece of information, comes down to the protective devices built into operating systems which work on the access control

principle. Other software solutions of more complementary nature include: firewalls, anti-virus programs, anti-spyware, anti-advertising or anti-spam software. Solutions for identification and authentication of the authorized entity (passwords, access codes or content filtering which is characteristic of the parental control) are also gaining popularity (Siwicki, 2013).

People are and always will be the pillar of cyber security. Unfortunately, they are also the weakest link and criminals are well aware of it. Human mistakes arise from routine, negligence, misuse of technology and from insufficient knowledge on threats. Criminals using a rich arsenal of social engineering are able to gain certain amount of control over human behaviour and consequently, are able to break even the most advanced technical security measures.

V. CONCLUSIONS

Cyberattacks affect countries, international organizations, corporations, enterprises and individuals alike. Criminal activities in the cyberspace include theft, burglary, sabotage, espionage, surveillance, destruction or modification of data and even fraud. One should not forget the threats of cyberterrorism or even cyber war. Cyber security can therefore be considered as a kind of a new challenge for the 21st century. That is why, there are more and more voices about the need to seal security systems, introduce new legal regulations, take decisions at the international level concerning initiatives aimed at educating societies about security in the cyberspace.

The internet community is, without doubts, a form of information society. Threats related to the cyberspace cannot be easily identified and classified in a closed catalogue. Continuous technological development makes it extremely difficult to control the cyberspace. The dynamism of changes in this area and the global range of the Internet translate into enormous regulatory challenges. The development of the information society requires the creation of appropriate legal base. However, the architecture of the cyberspace makes it necessary for this legal base to be of international nature because in the past many efforts undertaken on national level proved insufficient. The new legal system dedicated to the cyberspace should regulate effectively and comprehensively both information society issues and potential threats in the virtual space (Worona, 2017). Due to the increasing role of ICT systems in the society and also in the state infrastructure, the cyberspace has become the subject of interest not only of the contemporary legal doctrine, but also of scientific thought. The new digital environment not only has had impact on the conclusion of civil law contracts or administrative activities but also contributed to the emergence of new forms of crime. Therefore, this environment must be under strict scrutiny because along technological progress, new forms of threats for cyber security will emerge and, as a consequence, new counteractive measures will have to be invented.

VI. REFERENCES

Adamski A., Prawo karne komputerowe, C. H. BECK, Wrocław 2000, p. XVIII.

Barta J., Markiewicz R., Prawo cyberprzestrzeni i stare konwencje [in:] "Rzeczpospolita" 15 November 1997, no 266.

Białoskórski R., Cyberzagrożenia w środowisku bezpieczeństwa XXI w. - zarys problematyki, Warszawa 2011, p. 13.

Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cybercrime, Brussels, 22.5.2007, COM(2007) 267 final.

Czechowski R., Sienkiewicz P., Przestępcze oblicza komputerów, Warszawa 1993, pp. 133-134.

https://www.computerworld.pl/news/Cyberbezpieczenstwo-co-powinienes-wiedziec-by-skutecznie-chronic-swoja-firme-przed-cyberatakami,404323.html (access 14 January 2019).

https://www.polskaszerokopasmowa.pl/technologie/artykuly/klucz,jak-sie-bronic-przed-cyberatakami-o-dlugotrwalym-dzialaniu,akcja,pdf.html (access 14 January 2019).

Johnson D. R., D. G. Post: Law And Borders - The Rise of Law in Cyberspace, Stanford Law Review no 48 (1996).

Kronke H., Applicable Law in Torts and Contracts in Cyberspace [in:] Which Court Decides? Which Law Applies?, The Hague, London - Boston 1998, p. 65.

Post J., Law and Order – Cybercrime: Information and People, 2009, p. 1367.

Sienkiewicz P., Ontologia cyberprzestrzeni, Zeszyty Naukowe WWSI 2015, no 13, vol. 9, p. 98.

Sienkiewicz P., Świeboda H., Niebezpieczna przestrzeń cybernetyczna, Transformacje 2006, vol. 47-50, p. 58, based on: J.A. Warden, The Enemy as a System, „Air Power Journal" 1995, vol. 9, no 1, pp. 90-92.

Siwicki M., Cyberprzestępczość, C.H. Beck, Warszawa 2013, pp. 80-81.

Siwicki M., Nielegalna i szkodliwa treść w Internecie. Aspekty prawno karne, Wolters Kluwer Polska, Warszawa 2011, p. 258.

Świerczyński M., Koncepcja autonomicznego prawa cyberprzestrzeni [in:] Prawo Internetu, LexisNexis, Warszawa 2004, p. 164.

The North Atlantic Treaty Organization signed in Wahington on 4th April 1949.

Trelikowski M., Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm, [in:] M. Madej, M. Trelikowski, Bezpieczeństwo teleinformatyczne państwa, Warszawa 2009, pp. 96-97.

Worona J., Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy, Uniwersytet w Białymstoku, Białystok 2017, p. 65.

Wójcik J. W., Cyberprzestępczość. Wybrane zagadnienia kryminologiczne i prawne, „Problemy Prawa i Administracji" 2011, no 1, p. 155.