Stanisław Hoc

CYBER TERRORISM – THREAT TO THE SECURITY OF THE STATE AND ITS CITIZENS

1. Introductory notes

The issue of cyber crime, including cyber terrorism, has in recent years become the interest of doctrine, legislation and legal practice.[1]

Development in information technology as well as in IT – related infrastructure has led to the growth of cyberspace as a new area of social activity. It is assumed that this term defines all instances of virtual (non–spacial) communication in a physical, immaterial and non–geographical sense, which has been generated due to information technology and its physical manifestation (computers and telecommunication infrastructure).[2]

According to M. Madej[3] the characteristics of cyberspace conceived in this way differ from the characteristics of physical reality, which determines the different nature of any activities taken in its area. This difference will depend mainly on the following factors: low and steadily decreasing cost of initiating and carrying out activities that are taken in cyberspace, regardless of geographical limitations and the relatively high level of anonymity afforded to anyone who undertakes such attack or any other wrongdoing.

It needs to be emphasized that cyber crime, unlike criminal law, has no national borders. Global communication infrastructure such as the Internet facilitates cross–

1 A. Adamski, Cyberprzestępczość – aspekty prawne i kryminologiczne. „Studia Prawnicze" 20005, issue 4 (166) and other works of the above author, Cyberterroryzm nowe wyzwania XXI wieku. Collective work edited by T. Jemioła, J. Kisielnicki and K. Rajchel. Warsaw 2009, J. Kosiński, Conferrence summary „Przestępczość w cyberprzestrzeni" (15–16 December 2009 Toruń). „Przegląd Policyjny" 2010, issue 1(97), p. 178–181, A. Suchorzewska, Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem. Warsaw 2010.

2 A. Bógdał–Brzezińska, M.F. Gawrycki, Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie. Warsaw 2003, p. 37–39.

3 M. Madej, Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państwa i systemu międzynarodowego (in:) Bezpieczeństwo teleinformatyczne państwa. Edited by M. Madej i M. Terlikowski. Warsaw 2009, p. 29.

border crime and allows simultaneous harm to be caused to a number of users in many countries with a single act which may not necessarily be penalized in the perpetrator's country of domicile.[4]

It is probable that leaving such crime beyond exterritorial jurisdiction originates from the assumed relatively low harmfulness of cyber crime, which is not perceived by legislators as a source of real threat to public (over individual) good like state security or the conventional telecommunication infrastructure.

From a legal comparative point of view it becomes clear that some legislators do not adhere to the above mentioned conviction.

A good example can be seen in Polish criminal legislation, in which the crime of 'computer sabotage' (act 269 § 1 and 2 Penal Code) being an action against IT data of 'special importance for the state's defence system' is subject to Polish jurisdiction on the grounds of protection (act 112 Penal Code) e.g. in case an electronic attack on computer–supported elements of Poland's anti–missile system is accomplished from the territory of a 'hacker friendly' country. Since the telecommunication infrastructure is considered to be the world's Achilles's heel, legislation in the USA, the country having the best developed systems, goes even further in such regulations.[5]

Polish criminal legislation pays special attention to crime against data protection (ch. XXXIII Penal Code).[6] It is assumed that legal grounds for fighting Internet crime are enacted in the areas of consumer rights, data protection, telecommunication law and criminal law.

The term 'cyberterrorism' came into use in the USA in the late 1990's, followed by a variety of definitions, which is why there is no one definition which can be described as consistent and generally accepted.[7]

M. Terlikowski[8] assumes that cyberterrorism means terrorist activity in which electronic programmes and devices are used as tools or weapons in the hands of terrorists. The act of cyberterrorism (in strict understanding) is an electronic attack which is an element of terrorist combat and results in significant physical damage (other than damage to computer hardware) or even human casualties. The author believes that an attack can be considered an act of cyberterrorism if it is immediately

4 A. Adamski, Podstawy jurysdykcji cyberprzestępstw w prawie porównawczym (in:) Księga pamiątkowa ku czci Profesora Jana Białocerkiewicza. Volume. 2, edited by T. Jasudowicz and M. Balcerzak. Toruń 2009, p. 937

5 A. Adamski, *op. cit.*, p. 954–955.

6 S. Hoc, Karnoprawna ochrona informacji. Opole 2009, p. 13 and following., B. Kunicka–Michalska, ch. XXXIII. Przestępstwa przeciwko ochronie informacji (in:) Kodeks karny. Część szczególna. Komentarz do artykułów 222–316. Volume II. Edited by A. Wąsek, R. Zawłocki, 4th edition, Warsaw 2010 r., p. 540–749.

7 G. Weimann, Terror on the Internet. The New Arena, the New Challenges, Washington 2006, p. 152–154.

8 M. Terlikowski, Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm (in:) Bezpieczeństwo teleinformatyczne państwa, *op. cit.*, p. 111.

connected with a particular political issue and the perpetrators make a clear statement that the attack is a form of struggle for their cause.

Development in information technology and IT–based infrastructure leads to the growth of cyberspace being a new area of social activity. This term refers to a variety of virtual relations generated due to information technology as well as its physical manifestation (computers and telecommunication infrastructure).

The term 'cyberspace' has been supposedly coined by the American science – fiction writer William Gibson, the author of a literary trend called cyber–punk, who was the first to use this concept in his novel 'Neuromancer' published in 1984 (Polish edition, Warsaw 2001).

2. Threats in the Internet and in other areas

It is worth noting that the Internet can be used for criminal operations. The Internet was created in the 1960's. The first telecommunication network, created in the USA in 1969, was ordered by a military agency ARPA (Advanced Research Project Agency, presently known as DARA (Defense Advanced Research Agency, which was established in 1972 following the reorganization of ARPA) and was designed to test the potential of designing and building a net structure capable of functioning without a specific central point and after sustaining damage to any part of it. In Poland the Internet was first used on 17 August 1991, when scientists from the Faculty of Physics of Warsaw University, exchanged emails with the Computer Centre of the University in Copenhagen. On 20 December 1991, the USA abolished restrictions on computer connection with Poland, as a result of which Poland joined the global Internet.[9]

The Internets users are: administration (including government and self – government bodies), businesses and individual users. The Internet is exposed to various operations which directly or indirectly threaten telecommunication security (threat to the state and its citizens).

Threats to telecommunication security (apart from the effects of natural and technical disasters) comprise remote controlled and unauthorized operations in telecommunication systems, the aim of which is to block or disturb their functions, take over their control or obtain data they contain.

Such operations (electronic attacks) can be targeted at telecommunication systems which belong to public administration, corporations or individual users.

9 P. Dawidziuk, B. Łącki, M.P. Stolarski, Sieć Internet – znaczenie dla nowoczesnego państwa (in:) Bezpieczeństwo teleinformatyczne państwa, *op. cit.*, p. 41 and following.

Attention should also be paid to threats of computer crime resulting from the activities of hackers. In Poland, there have as yet not been any instances of spectacular acts of sabotage or attacks on IT systems, however such cases are likely to happen in the very near future.

According to the report prepared by the American company, Symantec for the second half of 2006 (Symantec Internet Security Threat Report. Trends for July – December 06, www.symantec.com) Poland ranks third in the number of incidents per one Internet user which shows that the Polish Internet is significantly exposed to various infringements of telecommunication security. For instance, in 2005 the website of the weekly 'Tygodnik Powszechny' was blocked for two hours as a result of attack. Portal 'gazeta.pl' was also attacked by 80 thousand so called 'zombie computers' from Latvia, Russia, Spain, Iran and Asian countries. The website of the Atomic Energy Institute in Świerk was repeatedly hacked to insert a supposed Al–Qaida terrorists' announcement. In May 2007, the home website of the Police was blocked and in August 2007, the Internet system of visa applications was attacked at the Polish Consulate in Lviv. When in June 2008, the Internet hypermarket Max.24. pl from Nowa Sól was attacked by cybercriminals, this crime was reported to the prosecutor's office in Zielona Góra on grounds of art. 269a, Code of Penal Law.

Criminals often make use of so called 'zombies', that is infected computers of which they take control without their owners' awareness. This army of 'zombie' computers is then given an instruction to connect with a particular website causing the service it provides to collapse.

It needs to be explained that DoS (Denial of Service) stands for an attack on a computer system or an internet service which disables its function through data overload and the occupation of all free data processing resources.

On the other hand, DDoS (Distributed Denial of Service) stands for a dispersed attack which blocks a service, another method used by cybercriminals and which is aimed at blocking network devices.

SPAM is a term which can be defined by reference to quantity which is, sending with the use of electronic communication media, large numbers of bits of information with the same content to recipients who are not known to a sender (mass correspondence). The category of spam encompasses unsolicited commercial offers as well as non–commercial messages, e.g. petitions from social or charity organizations, presentations of political parties or warnings against computer viruses sent in mass copies. The basic method of protection against spam distributed by email is black–listing.

From the perspective of state security, the areas which are most exposed to electronic attacks are energy resources (gas, electricity), transport systems (airports,

railways), manufacturing (factories), the output of raw materials and the emergency services (police, fire brigade, medical).[10]

Criminal law can play a subsidiary role in this area, with priority given to anti–hacking prevention and other measures taken by owners and users of IT equipment.

It is interesting to take a detailed look at the 2007 electronic attack on Estonia.[11] Perpetrators of electronic attacks are commonly referred to as 'hackers' and their operations as 'hacking'. Political relations between Estonia and Russia from the end of April to the middle of May, remained in serious crisis. This started after the Estonian authorities decided to move graves of Red Army soldiers killed during World War II – along with a monument commemorating them – from the square in Tallinn to a military cemetery. Since the monument, called the Bronze soldier, was for the Estonians a symbol of Soviet occupation and for the Russians and Russian minority in Estonia (20% of population) a symbol of a great military feat, a severe political conflict developed. The conflict was accompanied by a series of electronic attacks which seriously disrupted Estonia's telecommunication infrastructure. Estonia leads Europe in terms of intensive use of the Internet in everyday life. The first wave of electronic attacks, mostly blocking services (DDoS), took place on 27 April 2007, and affected the servers of Estonian government websites. Official websites of the President, the government and the parliament were also repeatedly blocked, and the websites of some prominent newspapers and TV stations attacked in a similar fashion. Under the attack these websites were temporarily inaccessible from the outside and their administrators were not able to control content. Members of Parliament were also cut off from effective channels of online communication when their email addresses were blocked. Hackers who broke into the website of the Estonian Reform Party, published a fake letter supposedly written by the Prime Minister. In this situation the Estonian authorities asked both the EU and NATO for assistance. Attacks remarkably grew in intensity on 9 May, the anniversary date of the Red Army victory in World War II, when servers of the second biggest Estonian bank (SEB Eesti Uhispank) were attacked blocking all online operations for several hours. However, websites of the country's authorities remained the main target and the scale of attack as well as its technical character, affected many other crucial servers nationwide. Computers which maintain the Estonian Internet system, were, for a couple of hours, flooded with amounts of data which way exceeded their capacity and which blocked the infrastructure. In order to prevent the collapse of the Internet system, international connections were cut off and access to the network was limited to non–urban areas of the country. This action weakened the overall impact of the attack, but internet resources remained inaccessible from abroad and

10 *Ibid.* p. 55.

11 M. Terlikowski, Ataki elektroniczne na Estonię. Implikacje dla bezpieczeństwa międzynarodowego i Polski. „Polski Przegląd Dyplomatyczny" 2007, issue 4, p. 53–74.

from areas located away from major cities. After 18 May, harmful attacks were not repeated. The campaign of electronic attacks was scheduled to last for a period of about three weeks and consisted of moments of intense activity and periods of relative calm. In January 2008, in the first trial of one of the attackers, an Estonian court fined a student, D. Galushkievich – a representative of the Russian minority – who coordinated attacks on the Reform Party's website. Galushkievich pleaded guilty, explaining that his action was meant to express political protest.

According to M. Terlikowski, the case of Estonia may be qualified as an example of "hacktivism" (hacking motivated by political beliefs and used as a method of expressing protest against politically related issues). Most electronic attacks emanated from Russia. However, Russian authorities denied cooperation in this area. NATO decided to establish the Tallinn based centre of cyber defense which came into being on 1 January 2009. The research and training centre in Estonia's capital, deals with issues of cyber security (Cooperative Cyber Defense Centre of Excellence). In 2008, NATO defined its cyberspace defense policy and appointed authorities responsible for managing and coordinating its member states' programmes in the area of cyberspace defense – NATO Cyber Defense Management Authority (CDMA). In each of the member states, NATO appointed a so called Focal Point to coordinate operations in case of the threat of a computer attack. In Poland this is the Telecommunication Security Department of the Agency of Domestic Security (ABW) with an adjunct in the Ministry of National Defense (MON). In NATO telecommunication security is coordinated by Communication and Information System Services Agency (NCSA) set up after the summit in Prague in 2002. Within the structure of the EU, there is the European Network and Information Security Agency (ENISA) created on 10 March 2004, in accordance with regulation 460/2004 of the European Parliament and EU Council. The role of the Agency is to strengthen the ability of the EU economy to resist threats and to react to the issues of tele–information security and to support the European Commission, along with member states, in all above mentioned problems. Its role is also to stimulate legislation and best practices in this area.

The EU responded to the situation in Estonia in its communication of 22 May 2007, (COM 2007 267 Towards a general policy on the fight against cyber crime 22 May 2007), where, apart from recommendations to fight Internet crime more effectively, there were also statements emphasizing the need to take measures preventing coordinated mass attacks on the IT infrastructure of member states. According to this announcement EU member states would discuss methods of exchanging information as well as good practices in this area and coordination of their reactions to such attacks. In the opinion of V. Reding, EU commissioner of information society, the Union should more intensively cope with the problems of tele–information security since the case of Estonia is a warning which has to make governments aware of how serious the threat is.

According to ENISA, operations by cybercriminals may soon threaten the EU economy. The agency claims that within the Union, six–million infected computers exist in networks that can be used for electronic attacks or sending spam. The losses suffered as a result of this by European companies is estimated to be 65 million Euros a year. The agency points out that the awareness of such threats is especially low among small and medium sized companies which account for two–thirds of the EU market. IT networks of those companies are now the weakest link of the Internet infrastructure and could be used for a spectacular attack. According to M. Kleiber,[12] events in Georgia showed that computer networks became the key element of a deceitful struggle with potentially serious consequences. Starting from 20 July, government servers in Georgia were attacked with messages including a phrase 'win+love+in+Russia'. Simultaneously, and with the same methods of electronic attack used in Estonia, hackers blocked servers of the President of Georgia, the Ministry of Foreign Affairs and the Ministry of Defense. Georgian services had to be moved to servers abroad. In the opinion of American specialists, the attack on Georgian websites was carried out with the participation of Russian Business Network – a hacker group set up in 2006 and which in 2007, was responsible for 60% of the world's cybercrime. It is worth noting that cybercriminals have millions of computers at their disposal worldwide and use them in espionage, disturbing air traffic, damaging energy installations by unfair competition and terrorism. It has now become necessary to take effective measures of prevention and repression such as forming special units to monitor and prevent threats, international coordination of their activities and the support of studies on modern tele–information methods. Studies in cryptography, software engineering, risk management or psychology of crime and their commercial implementation, is the key to the future security of tele–information networks – underlines M. Kleiber. Kleiber, also observes that cybercriminals are often well educated IT specialists capable of breaking any protection system but which, however, requires a certain amount of time. The thing is that we need to be ahead of them and 'delay the chase' by restrictive punishment for those criminals identified. The incidents in Estonia and Georgia showed that a properly selected and well equipped group of cybercriminals – hackers, within a couple of months would be able to prepare a number of electronic attacks such as sabotage and network vandalism, which means destroying data and services or theft of assets or identities. Collectively, these acts could have very negative influence on the security of the whole country.

On 21 January 2010, H. Clinton, Secretary of State in B. Obama's administration, announced the launch of a new programme called 'Freedom of the Internet' directed against the censorship of electronic information which is a practice in some

12 M. Kleiber, Wojna zaczęła się w sieci, „Rzeczpospolita" 2008 of 2 September.

countries. This declaration was the effect of events at the end of 2009, when the electronic resources of the Google website stored on US based computers, were electronically broken into, presumably on Chinese inspiration. The aim of the attack, was to obtain from gmail.com (email service offered by Google), the email addresses and record of keywords typed into search engines by users suspected of subversive activities against the Chinese government. In the middle of January 2010, The USA demanded an explanation from China concerning the attacks on Google and asked for investigation to identify the culprits and to bring them to justice under national jurisdiction.[13]

H. Clinton claimed that if companies' interests were to threaten freedom of speech, they should carefully analyze their motives and choose what is right instead of placing profits first. She also expressed her hope that denial of support for political censorship, would become the trademark of new American technology firms. Clinton gave assurance that the American administration would support the development of Internet tools which enable citizens to make use of their freedom of speech.

J. Kulesza,[14] is right when he criticizes the Chinese practice of Internet censorship. He believes, however, that filtration of Internet content is not necessarily unacceptable. The Internet is flooded with content that should not be propagated since it is dangerous and harmful. The global network will need security standards in order to protect users from such threats. Therefore, for the sake of the global Internet, we need to take the challenge of setting minimum standards of worldwide censorship. J. Kulesza,[15] emphasizes the fact that in order to reach international agreement, the issue of Internet filtration should begin from the common ground for all national policies: protecting citizens from terrorism, sexual crime and weapons of mass destruction. It is necessary to establish international authority that will give shape to standards of freedom in the network. There is no question that the issue is difficult and complex but the Internet has forced the international community to face the need of setting global standards of human rights.

In Poland the awareness of the importance of tele–information security is growing very slowly, however, the government is taking some measures in this area but there is still no complex approach to the issue of threats. According to sources,[16] problems of incidents in computer networks remain within the capacity of the Computer Emergency Readiness Team or the Computer Emergency Response Team (CERT). Handling security incidents in particular is the responsibility of the Computer Security Incident Response Team (CSIRT). Such teams are set up

13 J. Kulesza, Amerykańsko–chiński spór o cenzurę w Internecie. „Państwo i Prawo" 2010, issue 6, p. 29 and following.
14 *Ibid.*, p. 39.
15 *Ibid.*, p. 41.
16 M. Szmit, I. Politowska, Artykuł 267 kk. oczami biegłego, „Monitor Prawniczy" 2008, issue 16, app., p. 36.

by institutions managing large computer networks in order to investigate incidents threatening security and give assistance to users. CERT Polska, operates within Scientific and Academic Computer Networks. CERT teams cooperate within the Forum of Incidents Response and Security Teams (FIRST), however membership in FIRST is not obligatory.

The Government Computer Incidents Response Team CERT.GOV.PL was established on 1 February 2008, within the Internal Security Agency (ABW). Its aim is to create policy in the area of cyberthreat security, to coordinate the flow of information between institutions, to detect and recognize cyberthreats and to prevent them, to cooperate with national organizations and government institutions in the area of cyberspace protection, and to represent Poland in international relations (within its competence). The tasks of CERT.GOV.PL are: collecting information on security level and threats to tele–information infrastructure; responding to incidents of threat to tele–information security with special attention to the National Tele–information Infrastructure; using instruments of investigation IT to analyse incidents, forming the policy of tele–information systems and networks protection; training and raising awareness related to cyberthreat, and consulting on cybersecurity. Services rendered by CERT.GOV.PL, include: coordination of responses to incidents; publication of alerts and warnings; handling and analysing incidents (including collecting evidence by expert witness teams); publication of announcements (security bulletins); coordination of responses to gaps in security; handling incidents in networks protected by the ARAKIS–GOV system and carrying out security tests. Internal Security Agency (ABW) cooperates with the Scientific and Academic Computer Network (NASK) as well as with the CERT Polska team. In effect of this cooperation, ARAKIS–GOV – a passive early warning system against internet threats – has been implemented in over 60 state institutions.

The director of Government Security Centre (acting on the grounds of the Act of 26 April 2007, on crisis control) coordinates working out a Report on threats to national security and submits this Report to the Council of Ministers every second year. The Report includes characteristics of terrorist threats that may lead to a situation of crisis (this part of the Report is coordinated by the head of Internal Security Agency).

On 9 March 2009, the Standing Committee of the Council of Ministers, accepted 'the government programme of Polish cyberspace protection in 2009–2011' which breaks into five parts (introduction, organizational and legal operations, technical operations, social and specialist education, summary). The programme defines cyberterrorism as terrorism directed against systems that are crucial for the state, tele–information networks and services, being a key and still increasing form of terrorist attacks. Cyberspace is defined as space of communication created by a system of

Internet connections. The programme presents aims and methods of realisation. The programme is directed at public administration and other institutions managing the state's critical resources of tele–infomation infrastructure. The programme is realised by the Ministry of Internal Affairs and Administration, Internal Security Agency, Ministry of National Defense, Military Counter–Intelligence, and other institutions of public administration and private organizations that are in possession of resources crucial to the state's tele–information infrastructure. Implementation of the programme is coordinated by the Minister of Internal Affairs and Administration whereas the Minister of Internal Affairs and Administration, Minister of National Defense, Head of Internal Security Agency, Head of Military Counter–Intelligence and other institutions of public administration, act according to their capacity. The programme assumes organizational and legal attempts aimed at the legal definition of terms referring to cyberspace and cyberterrorism.

3. International legal regulations

The problems of fighting computer crime are remarkably recognized by EU conventions and legal acts. Under the Council of Europe, an international convention was formulated, accepted in Budapest and submitted for ratification on 23 November 2001.[17]

The Convention on cybercrime came into force on 1 July after five ratifications including three ratifications by Council of Europe member states to accord with requirements specified in Art. 36.

The Convention on cybercrime concerns four categories of crime: crime against confidentiality, integrity and accessibility of information data and systems (illegal access, illegal takeover of data, infringement of data integrity, infringement of system integrity, inappropriate use of equipment); computer crime (computer forgery, computer fraud); crime in terms of the content of information (child pornography), and crime related to the infringement of copyright and intellectual property right. A further category of crime committed with the use of information systems was defined in the protocol amendment on cybercrime ratified in Strasbourg on 28 January 2003. It deals with the criminalization of any racist or xenophobic acts committed with the use of computer systems.[18]

17 R. Tarnogórski, Konwencja o cyberprzestępczości – międzynarodowa odpowiedź na przestępczość ery informacyjnej (in:) Bezpieczeństwo teleinformatyczne państwa, *op. cit.*, p. 205 and following.

18 M. Urbańczyk, Protokół dodatkowy do Konwencji o cyberprzestępczości jako przykład europeizacji prawa karnego (in:) Prawo wobec wyzwań współczesności. Volume V. Edited by B. Guzik, N. Buchowska and P. Wiliński. Poznań 2008, p. 409 and following.

The EU Act of fundamental significance is the Framework Decision 2005/222/ WsiSW of 24 February 2005, dealing with attacks on information systems, and which contains legal acts of material law of similar range of regulation to the Convention on cybercrime. In the Decision, harmonization is presented as a need to reach a common approach in reference to elements of crime by defining the crime of illegal access to information systems and illegal interference with data. As yet, regulations assumed in the Decision and the Convention are not identical.

The conclusions of the EU Council on fighting cybercrime accepted during the meeting on 27/28 November 2008, in Brussels, proclaim amendment to the above framework decision and a call for the elaboration of overall EU strategy in fighting cybercrime considering the achievement of the Convention on cybercrime. This strategy is not a new idea, the Communication to the European Parliament, the Council and the Committee of the Regions, titled 'Towards the general policy on the fight of cyber crime' (52007DDCo267 COM/2007/267 final) advocates implementation of political measures in order to improve the coordination of fighting cybercrime on a European and global level. The above mentioned Communication in a synthetic way comprises the EU Commission's position towards the issue of cybercrime. This term is defined as 'criminal acts committed by means of electronic communication networks and information systems or directed against such networks or systems.

The common term cybercrime comprises three categories of crimes:

- traditional types of crime (fraud, forgery) committed with the use of electronic information networks and information systems (in this communication referred to as electronic communication networks)
- publication of illegal contents by means of electronic communication media, i.e. the circulation of child pornography
- crime typical of electronic communication networks, i.e. hacking and DoS and DDoS – type attacks on information systems and hacking.

The European Commission also justifies the necessity to elaborate EU policy on fighting cybercrime. The Commission and member states set further development of EU policy as the main objective. This initiative will concentrate on fighting crime and on aspects of criminal law and this strategy being to complement other EU activities to improve overall security of virtual space. The strategy will comprise: better operational cooperation of law enforcement authorities, better political coordination between states, political and legal cooperation with third countries, raising awareness, supporting training and research, improving dialogue with the industry sector and activities in the area of legislation.

The Communication presents the existing legal instruments and activities taken within EU policy. The Communication also includes a vital declaration: considering the significance of the Convention on cyber crime as the most important European and international instrument in the area of cyber crime, the Commission decided to encourage member states and relevant third countries to ratify the Convention and to consider the possibility to join the Convention by the European Community, which would doubtlessly strengthen this legal act.

Poland as yet has ratified neither the Convention on cyber crime nor the protocol amendment but much has already been done to protect Polish citizens against cyber crime (amendments of Penal Code). Poland is considered a state which to a great extent has adjusted its legal system to existing standards in this area but this hypothesis is questioned in legal doctrine.[19]

4. Summary

Threats to cyberspace are real and result from crime, harmful content on the Internet, dynamic growth of viruses, faulty software, flood of spam and hacking attacks. Therefore there is a growing need for taking actions to prevent these phenomena and providing instruments which ensure security of the state and its citizens. The above mentioned actions are already in progress through legislation, organizational changes, changes in competences, and adaptation of the Polish legal system to international regulations. The implementation of Programme of the Government of the Republic of Poland gives hope for further improvement in the area of the country's cyber security.

19 A. Adamski, Cyberprzestępczość – aspekty prawne i kryminologiczne. „Studia Prawnicze" 2005, issue 4(166), p. 53.

CYBERTERRORYZM – ZAGROŻENIE DLA BEZPIECZEŃSTWA PAŃSTWA I OBYWATELI

Rozwój technologii informatycznych, a także związanych z infrastrukturą IT doprowadził do powstania cyberprzestrzeni jako nowego obszaru dla działań społecznych. Należy podkreślić, że cyberprzestępczość, w przeciwieństwie do prawa karnego, nie zna granic państwowych. Globalna infrastruktura komunikacyjna, taka jak Internet, umożliwia przestępczość transgraniczną i pozwala w tym samym czasie wyrządzić szkodę szeregowi urzytkowników z wielu krajów przez działanie, które niekoniecznie musi być przedmiotem penalizacji w kraju sprawcy.

Zagrożenia dla cyberprzestrzeni są prawdziwe i wynikają z przestępczości, szkodliwych treści w Internecie, dynamicznego zwiększenia ilości wirusów, złego oprogramowania, powodzi wiadomości–śmieci i ataków hakerów. W związku z tym istnieje rosnąca potrzeba podjęcia działań zmierzających ku zapobieżeniu tym zjawiskom i ku przyjęciu instrumentów, które zagwarantują bezpieczeństwo państwa i jego obywatelom.

CYBERTERRORISM – THREAT TO THE SECURITY OF THE STATE AND ITS CITIZENS

The development of information technology as well as in IT– related infrastructure, has led to the growth of cyberspace as a new area of social activity. It needs to be emphasized that cyber crime, unlike criminal law, has no national borders. Global communication infrastructure, like the Internet, enables cross–border crime and allows simultaneous harm to be caused to a number of users in many countries with a single act which may not necessarily be penalized in the perpetrator's country of domicile.

Threats to cyberspace are real and result from crime, harmful content on the Internet, dynamic growth of viruses, faulty software, flood of spam and hacking attacks. Therefore there is a growing need for taking actions to prevent these phenomena and providing instruments which ensure security of the state and its citizens.

Key words: cyberspace, terrorism, Internet, crime, security