MODERN MANAGEMENT REVIEW **2017**
MMR, vol. XXII, 24 (3/2017), pp. 141-152 **July-September**

Izabela OLEKSIEWICZ[1]

A LEGAL ASSESSEMENT OF MANAGEMENT OF THE EUROPEAN UNION CYBERTERRORISM POLICY

In addition to traditional threats such as spying or revealing state or business secrets, the new threats have appeared, among which the most dangerous is cyberterrorism. Proper functioning of society depends today largely on management functioning of modern techniques and information technology. Computers networks are widely used in economy, administration, as well as inhouseholds. Taking into account the problems of cyberterrorism, in particular an analysis of legislation aimed at ensuring the security of information systems of individual countries, this subject should be also recognized as a requirement for the insightful analysis.
Therefore, this publication is an attempt to characterize the determinants of this phenomenon and an analysis of the latest legal solutions in the fight management against cyberterrorism in the European Union. Moreover, an attempt has been made to present the EU counter-terrorism policy so the Author`s intention is also to show the impact of legal instrument on combating cyberterrorism itself. In addition, it tries to find an answer to the question whether the current legal standard solutions of the European Union in the area of security are an effective tool in the fight against cyberterrorism.

Keywords: management, cyberterrorism, policy, EU, law.

1. THE NOTION OF CYBERTERRORISM

Cyberterrorism has become a fashionable notion, but few people know what it really is. Many believe that this is only a theoretical concept, an action which probably will never happen in reality. But no one knows what the future holds.

The cyberterrorism was also defined by M. Pollite as deliberate, politically motivated attacks carried out by non-state groups or clandestine agents against information, computer systems, software, and data.

The term “cyberterrorism” appeared for the first time in 1979 in Sweden in the report that showed computer threats. It covered any activity involving computers aimed at the destruction of ICT systems, supervisory and control systems, programs, data, etc., and consequently intimidation of the governments and the societies to exert psychological pressure, bringing to life-threatening as a result of considerable damage. In the 80s of the twentieth century this term was used by the American special services, pointing at the possibility of carrying out electronic attacks by the enemies of the United States. In 1998, at the Headquarters of the FBI the National Infrastructure Protection Center (NIPC) was created, whose task was to coordinate the collection of information about the threats,

[1] Izabela Oleksiewicz, Dsc, PhD, Associate Professor, Department of Security Science, Rzeszow University of Technology; e-mail: oleiza@prz.edu.pl.

responding to the threats or attacks on critical information elements of the infrastructure of the state.

Defining cyberterrorism as a combination of cyberspace and terrorism means that such an activity is associated not only with the hostile use of IT and the action in the virtual sphere, but it is also characterized by all constitutive elements of the terrorist activity[2]. This term refers to the unlawful attacks and threats against computer networks and the information. Their aim is to intimidate or coerce governments or people in order to achieve certain political or social benefits. In addition, in order to qualify an attack as a cyberterrorism attack, it should be made as a result of violence against people or a property, or at least as a cause of significant damage in order to induce fear.

It must be stated that the concept of cyberterrorism is used in the context of a politically motivated attack on computers, networks and information systems in order to destroy the infrastructure and intimidate or coerce the government and people of far-reaching political and social objectives[3]. This concept has been the object of greater interest since the 80s of the twentieth century, and the speculation on this subject was intensified after the attacks of 11 September 2001 in the USA. The typical threats concern the traffic control systems, the bank infrastructure, the energy and water supply systems, as well as personal database systems, and government institutions[4].

The abovementioned definitions show that cyberterrorism is understood in the world in two ways. According to the first concept, terrorism and cyberterror are distinguished merely only by the use of information technology to carry out the coup, while the second concept focuses on computer systems as a target of attacks, and not a tool to carry them out. It seems that the true definition arises only after the connection of of both approaches[5].

Cyberterrorism is defined as a form of use of telecommunications networks, computer networks and the Internet aimed at breaching of any good protected by law. Cyberterrorism differs from the classic crime primarily operating in an environment related to computer technology and the use of computer networks to commit crimes[6]. However, its distinguishing feature is not to protect anybody's common good[7]. Today, almost every illegal activity is reflected in the Internet. The global nature of the Internet allows extremely fast communication and the transfer of most forms of human activity to the network and these negatively received as well. More and more frequently one speaks of cyberspace as a new social space, which reflects the same problems as in the real world. Therefore, cybercrime

[2] The official website of Department of Computer Science in Georgetown 2016.

[3] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2006, p. 36.

[4] See also: A. Janowska, *Cyberterroryzm – rzeczywistość czy fikcja?* [w:] *Społeczeństwo informacyjne. Wizja czy rzeczywistość?*, Kraków 2004, p. 445–450.

[5] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem*, Warszawa 2010, p. 17.

[6] See: R. Białoskórski, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Warszawa 2011, p. 63; A. Gniadek, *Cyberprzestępczość i cyberterroryzm – zjawiska szczególnie niebezpieczne* [w:] *Cyberterroryzm. Nowe wyzwania XXI wieku*, red. T. Jemioło, J. Kisielnicki, K. Rajchel, Warszawa 2009, p. 333.

[7] *Ibidem*, p. 213.

is a modern alternative of crime, it exploits the possibilities of digital technology and the environment of computer networks[8].

This makes protection against the threats posed by cybercrime extremely difficult and requires taking a number of projects including a multi-faceted challenge and broad international cooperation. The effectiveness of this protective cooperation is essential for individual countries to establish a common policy against cybercrime and its concretization, specifying the priorities and uniform principles of joint action. These general rules need to be implemented into national law of a country and become the basis for institutional and functional system of tools to fight cyberterrorism. The creation of an effective system to counter cyberterrorism is not easy, and it requires a thorough analysis of the phenomenon in the long term, and the creation of such a system may encounter numerous problems in adapting the general guidelines of international or EU law into domestic law.

2. METHODOLOGY

This research implements an analytical doctrinal methodological approach. The doctrinal approach examines primary legal documents in order to draw a logical conclusion regarding the state of the EU law. The research examines the present status of existing regulations in the fight against cyberterrorism in the EU. An attempt was done to show how important element of internal security in the world today cyberspace is. An analysis presents EU cyberspace policy, hence the intention of the author was also to present the impact of the legal instruments to combat the cyberspace phenomenon and to propose new legal solutions designed to enhance cyberspace policy in the European Union, and thus the internal security of Europe today. This study also makes a review of the following documents:

Primary Documents

The key articles that this study reviews are as follows: Article 83 paragraph 1 of TFEU establishing the principle that within the EU law minimum rules concerning the definition of criminal offenses and sanctions in the areas of particularly serious crime of a cross-border nature can be established. Besides, Directive No. 2013/40/EU, Directive 2014/41/EU of the European Parliament is reviewed as the example of the legal instruments to combat the phenomenon of cybercrime.

Secondary Materials

This study reviews and evaluates different relevant secondary materials, among them those published in peer reviewed journals and also in some case studies.

3. THE EU INTERNAL SECURITY DETERMINANTS

Religious, demographic, social and ideological issues - apart from military and economic challenges – have become the main factors of crisis in Europe today. Undoubtedly, cultural differences, and especially religion are the main motive of various terrorist groups. A cultural factor can also be a kind of barrier to mutual understanding of the objectives and intentions, the consequence does not need to be a terrorist attack in the tradi-

[8] M.N. Schmitt (ed.), *The Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge University Press, 2015, p. 34–36.

tional sense. The source of aggravating these tensions may be the fact that the cultural and civilizational diversity are often used as a bargaining power in the event of a conflict, but in fact the source of the real reasons for their rivalry are quite different[9].

Globalization seems to be so advanced that a network of various relations between countries and societies in the world are too dense to be disintegrated or reduced. The inevitable consequence of globalization is the development of state sovereignty, which affects each of country, although to varying degrees. This is due to "deterritorialization" of the deepening interdependence of various global or international actions in every area of social life. This process takes place gradually, but is as durable as the globalization affecting in this way to an order and international environment[10].

The process of globalization, especially affecting the socio-economic sphere, creates new security risks. It is also important as a part of the crisis phenomena that take place outside its territory. It directly impacts on the internal situation of European countries and the European community. In the opinion of large sections of communities, to maintain security of employment and an adequate number of jobs, the appropriate level of social security and cultural identity should be a priority task of the state[11].

To find the answer to the question of what a cyber-war is, at the outset it is important to understand why IT networks are increasingly being used by governments? First of all, this is due to the specification of electronic signal path, and hence the same cyberspace. In cyberspace there are no traditionally understood boarders, although ICT infrastructure is located in specific countries. It is immaterial, but operates on the basis of the actually existing infrastructure and generates an electromagnetic field. Using this feature, one can get tangible material benefits.

With the immateriality of cyberspace other characteristics are related. First of all, the network is global[12]. As a consequence, the limitations of a physical character do not apply here. It is relatively easy to hide a real identity of the perpetrators of the incidents of ICT. There is a lack of not only strategic intelligence, but also, in many cases, the possibility of identification of the person responsible for the computer attack. This is contrary to appearance, the problem of fundamental importance. The identification of the subject responsible for the break-in is in an essential fact for the preparation of an appropriate political, judicial or military response.

Another important feature of cyberspace are relatively low operating costs. The development of conventional military capabilities are usually associated with very high financial outlays, including not only the training of personnel, but also the modernization and maintenance of equipment. Meanwhile, the tools that can be used to attack the ICT envi-

---

[9] Compare: R. Snyder, *Hating America: Bin Laden as a civilizational revolutionary*, "Review of Politics" No. 4/2003, p. 25–349; M. Madej, *Zagrożenie asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, PISM, Warszawa 2007, p. 86.

[10] J. Gryz (red.), *Zarys teorii bezpieczeństwa państwa*, Warszawa 2016, p. 107–128.

[11] Theoretically, one person could potentially make detriment, which in fact can be the result of the activities of organized terrorist groups or military units.

[12] It can wipe actors distant from each other by thousands of kilometers. Space ICT facilitated this practice by both state and non-state entities. Now, from the other end of the globe, with a relatively low risk of incurring the consequences, the relevant data can be almost instantly obtained, including, for example, document and technology of fundamental importance for national security.

ronment in this perspective, are almost free[13]. Cyberspace attacks make defense activities difficult. At the same time, as indicated above, the offensive actions are relatively cheap and easy to carry out. This feature of cyberspace is more noticed. The paradox can be noted. On the one hand, the use of ICT in all spheres of human life is associated with momentous benefits, for example, organizational, communication and financial position. At the same time it makes a technologically advanced body which is much more sensitive to attacks of ICT. In addition, as noted by Fred Schreier[14] ICT space is seen by many as a part of the common heritage of the mankind. In his opinion an important feature of the ICT is favoring offensive action over the defensive one.

The last group of reasons, due to which cyberspace has a growing interest in countries associated with the broader sphere of information, is ICT space because it has a huge potential from the perspective of propaganda or psychological operations. New information and communication technologies can be effectively used, e.g. to manipulate public opinion or disinform[15].

4. EU LAW TO CYBERTERRORISM POLICY

It should be emphasized that in the case of European countries, terrorism had primarily internal character. This has resulted in two kinds of consequences. Countries have recognized and still are saying that counter-terrorism is their exclusive competence. International cooperation in this regard perceive as necessary to fight the terrorism. At the European Union level, a qualitative change for the creation of tools to combat cyberterrorism took place in 2007. After the introduction of the Lisbon Treaty[16], internal security still belongs to the exclusive competence of a given country. In accordance with art. 2 sec. 2 TL is the area of freedom, security and justice that has fallen into shared competence. The basis for an action and in this area is the principle of entrusted competence: according to its content, the exercise of competences conferred on the European Union is subject to the principles of subsidiary and proportionality belong to the Member States. However, the principle of subsidiary has been clarified on the part of the Member States, and this principle is not only applicable to "central" countries but also "regional and local".

Criminal law has become a separate, though specific policy of cooperation, the new way for the harmonization of legislation in the field of substantive and procedural criminal law has been open[17]. Article 83 paragraph 1 of TFEU established the principle that within the EU law minimum rules concerning the definition of criminal offenses and sanctions in the areas of particularly serious crime of a cross-border nature can be established.

---

[13] State relatively easily may come into possession of malware (viruses, Trojans, worms), as well as the equipment needed to carry out even advanced operations. Increasingly, government agencies themselves are developing the most powerful tools, which do not involve, however, the major costs in terms of budget (the case of the Stuxnet virus).

[14] See more: F. Schreier, *On Cyberwarfare*, „DCAF Horizon 2015 Working Paper", Vol. 7, p. 11.

[15] An interesting manifestation of such measures were Russian cyber-attacks on Estonia and Georgia in 2007–2008. In both cases, limited opportunities for an active information policy for these countries helped to strengthen the position of the Russian Federation in the international arena.

[16] The Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community was drawn up in Lisbon on13 December 2007 (Journal of Laws of 2009, No. 203, item. 1569).

[17] Compare: M. Siwicki, *Cyberprzestępczość*, Warszawa 2013, p. 41.

At the same time, one clearly indicated that this was also about cybercrime. These are the forms of criminality in which Member States have already adopted minimum standards for the offenses or the scope of criminal penalties, in the form of framework decisions under the former art. 31 TEU in relation with art. 34 sec. 2 lit. B TEU. Adoption of minimum standards in areas other than those specified in this provision will require prior approval of the Council. So far, regional action was rarely taken or replaced at global level, especially within the UN framework.

So far, European states have focused on combating terrorism in Europe without going beyond its borders. Contemporary transformations of terrorism show that the role of religion is increasing at the motivational level, the tactics, methods and means used by terrorists change, resulting in greater heterogeneity of the phenomenon and forcing participants to cooperate with flexibility and rapid adaptation to the changes. The liquidity of the structures of the present terrorist organizations does not facilitate the counteracting of this phenomenon for contemporary states and international organizations.

An example of EU legislation on the problem of cybercrime is Directive No. 2013/40/EU[18] of 12 August 2013. It replaced the earlier Council Framework Decision 2005/222/JHA[19] of 24 February 2005 and it caused its development and refinement. The aim of the Directive is to improve cooperation between the competent authorities of the member states in the area of attacks against information systems and the establishment of minimum standards concerning the definition of criminal offenses.

According to the art. 2 of the Directive on attacks against information systems, "computer system" means any device or a group of connected or related devices in which one or more perform automatic processing of computer data, as well as computer data stored, processed, recovered or transmitted for the purposes of their operation, use, protection and maintenance. "Computer data" means any representation of facts, information or concepts in a suitable form for processing in a computer system, including a program suitable for causing performance of the functions of the system. The term 'unlawful' is defined as an access or interference for which the owner, or another right holder of the system has not given this consent, or which is not allowed according to law[20].

In order to standardize the legal systems it was recognized that in each member state an illegal access to the computer system, and illegal interference with the system and data should be treated as a crime. Illegal access to information system is understood as an intentional, unlawful access to all or part of the information system[21]. Member states are free to decide whether it is always covered by the indictment, or only when the offense is committed by infringing a security measure. Illegal system interference under article 4 of the Directive is unlawful, intentional serious hindering or interruption of the functioning

[18] Directive of the European Parliament and of the Council 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA(JOL EU L 218 of 14 August 2013.).

[19] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems (JOL EU L, No. 69, of 16 March 2005.).

[20] A.M. Kruk, *Bezpieczeństwo transferu informacji w XXI wieku w świetle bezpieczeństwa państwa i organizacji* [w:] S. Sulowski, M. Brzeziński (ed.), *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, Warszawa 2009, p. 345.

[21] F. Radoniewicz, *Postanowienia decyzji ramowej Rady w sprawie ataków na systemy informatyczne a ujęcie cyberprzestępstw w kodeksie karnym*, „Ius Novum" No. 1/2009, p. 48; A. Sakowicz, *Prawnokarne gwarancje prywatności*, Zakamycze 2006.

of the system by inputting, transmitting, damaging, deleting, destroying, altering, suppressing or rendering inaccessible computer data. In contrast, illegal data interference in accordance with article 5 of the Directive means the intentional and unlawful removal, damage, deterioration, change, suppression or rendering inaccessible computer data in a computer system[22].

According to art. 8 of the Directive on attacks against information systems, the following actions are also the subject of the penalty: help, an attempt and incitement to commit the aforementioned crimes. It is worth noting that each member state may decide that it will not be punished as a criminal during an attempt to gain illegal access to information systems. The offenses should be punishable for at least two years. This penalty is, however, aggravated if the acts of illegal interference in the system and data, as well as illegal access to the security breaches were committed as a part of a criminal organization or caused serious harm or affect the essential interests. Then they shall be punishable for at least three years of imprisonment. It was found that for the criminal liability not only the individual, but also a legal person could be held[23].

In the legislation of the European Union one can also find regulations related to the criminalization of activities aimed at disseminating information prohibited by law, including those via computer networks. The directive 2011/93/EU of 13 December 2011[24] contains the provisions on combating the sexual exploitation of children, including child pornography distributed through the Internet. It lays down minimum standards for the definition of criminal offenses and penalties related to sexual abuse, and sexual exploitation of children, children pornography and solicitation of children for sexual purposes. It also introduces provisions to improve prevention of this crime and better protection of victims as a result thereof (art. 1 of the Directive). In art. 5 of the Directive there are the provisions for offenses related to child pornography. As the Directive Council of Europe in 2007 they describe the criminalization of specific offenses, indicating the minimum statutory sanctions for their commission. In art. 5 paragraph 3 it was predicted the criminalization of knowingly obtaining access through information and communication technology, to child pornography, the action should be accompanied by a criminal penalty of a maximum of at least one year of imprisonment.

The latest Directive 2014/41/EU of the European Parliament and of the Council of 3rd April 2014[25]concerning the European Investigation Order (EIO) in criminal matters art.1 paragraph 1 of the directive defines the broader concept of EIO than that one which was contained in the Framework Decision 2008/978/JHA. In the current wording it means a judicial decision issued or approved by a judicial authority[26] "the issuing State"[27] to call

[22] K. Gienas *Systemy Digital Rights Management w świetle prawa autorskiego*, Warszawa 2008, p. 229.

[23] See also: K. Indecki, *Prawo karne wobec terroryzmu i aktu terrorystycznego*, Łódź 1998, p. 23; R. Zgorzały, *Przestępstwo o charakterze terrorystycznym w polskim prawie karnym*, „Prokuratura i Prawo" No. 7–8/2007, p. 35; art. 10 of the Directive.

[24] Directive of the European Parliament and of the Council2011/93/EU on combating the sexual abuse, sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/ JHA(JOL EU.L No.335 of December 17, 2011).

[25] JOL EU L 130 on 1.05.2014.

[26] In contrast, the executing authority is the authority competent to recognize an EIO and ensure its execution in accordance with this Directive and with the procedures applicable in similar domestic cases.

"the executing State"[28] to carry out one or several specific investigative orders to obtain an evidence.

The directive applies from 21st May 2014. By 22nd May 2017 member states shall take the necessary measures to meet its requirements. It replaces the existing so far rules ratified by Poland of the European Convention on Mutual Assistance in Criminal Matters of 1959 and the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union in 2000, as well as the Council Framework Decision 2003/577/JHA on the execution in the European Union of orders freezing property or evidence and the Framework Decision 2008/978/JHA on the European evidence Warrant[29].

The EIO, like the EAW of 2008 is another instrument based on the principle of mutual recognition. Thus, it facilitates cooperation between EU Member States, excluding the double criminality requirement in the list of crimes, including terrorism. Moreover, the procedure of their application is simple, steps are taken directly by the judicial authorities. However, the European Evidence Warrant in 2008 is often rated as a useless instrument because it requires certainty as to the presence of evidence in the requested state[30]. In connection with this new instrument or EIO, it covers almost all investigatives and does not have this requirement. These instruments are crucial in the fight against the use of the Internet for terrorist purposes as they allow rapid international cooperation.

The EIO mechanism was created to enable the courts, prosecutors and other investigative authorities direct transmission of requests for a specific proof, secure and search the property or hearing by videoconference. The judicial authority of the country, to which EIO was directed, has limited grounds for refusal of enforcement of such a request (e.g. due to national security concerns) and strict deadlines for its implementation. As a general rule European orders are seen in the same way as those issued by national authorities.

According to art. 3 of the objective range of the EIO governing each investigative action beyond creation of a joint investigation team and the gathering of evidence within such a team investigation, as provided for in art. 13 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union and the Council Framework Decision 2002/465/JHA unless these actions are being taken to implement art. 13 paragraph 8 of the Convention and Article 1, section 8 of the Framework Decision 2009/426/ JHA[31].

Therefore, in accordance with art. 4 EIO directive may be issued:

a) with respect to criminal proceedings which initiated a judicial authority or which may be brought before the judicial authority in the case of an offense under the law of the issuing state;
b) in proceedings brought by the authorities in respect of acts threatened with punishment under the national law of the issuing state, as they represent a violation of

[27] This means the Member State in which the EIO is issued (Art. 2 paragraph. 1 item a).
[28] This means the END executing Member State in which you want to perform a particular investigative measure (Art. 2 paragraph. 1 item b).
[29] JOL EU L 350 on 30.12.2008.
[30] N. *Catelan*, S. *Cimamonti*, J.B. *Perrier, La luttecontre le terrorismedans le droit et la jurisprudence de l`Unioneuropeenne*, Press Universitaires, Marsylia 2014, p. 135.
[31] JOL EU L 138 on 4.6.2009.

the law, and the decision may give a rise to proceedings before a court having jurisdiction in particular in criminal matters;

c) in proceedings brought by judicial authorities in respect of acts which are punishable under the national law of the issuing state, they constitute a breach of law, where the decision may give a rise to proceedings before a court having jurisdiction in particular in criminal matters;
d) in connection with proceedings referred to in point a), b) and c) which relate to offenses or infringements for which a legal person may be held liable or punished in the issuing state.

In addition, the issuing authority in accordance with art. 6 EIO of this Directive may do so only if the following conditions are met:

a) issuing the EEW is necessary and proportionate to the purpose of the procedure referred to in Article 4, taking into account the rights of the suspect or the accused; and
b) in a similar national case management to carry out the investigative measure(s) indicated(s) in the EIO is permissible under the same conditions.

However, when the executing authority has reasons to believe that the conditions referred to in art. 6, paragraph 1 have not been met, it may consult with the issuing authority on the so-called EIO why they were taken. After such consultation, the issuing authority may also decide to withdraw EIO.

5. CONCLUSIONS

The fact is that modern information systems, which form a part of the critical infrastructure of the country, require much more solid protection than it seemed a few years ago. The effect of a rapid technological development has become a strong dependence of the economy on IT systems. Nowadays, they control telecommunications, banking, energy supply, the air traffic system, a network of trains, control water supply and sewage disposal. We could say that the modern economy would cease to function without them[32].

The need for security seems to be self-evident truth. Some companies are aware of this fact, others unfortunately do not. Certainly protection systems can be improved through the introduction of new legislation providing good practices in the area of security. However, one needs to remember to set new rules, balance the need for security with the right to privacy[33].

All these features make that cyberspace is increasingly becoming a target of the country. Some of them already since the 90s of the twentieth century have developed its potential in this field. One can understand not only employed professionals and its infrastructures, but also the techniques and tools used in attacks ICT. Rightly, it has been recognized that in its present form cyberspace can be effectively applied to meet specific interests in the international environment.

Another regulation is EIO which introduced a simplified and harmonized legal framework for cooperation in the collection of evidence for transnational criminal proceedings or investigations. Cooperation between the European Union and the member states in the

[32] I. Oleksiewicz, *Ochrona praw jednostki a problem cyberterroryzmu*, HSS, Vol. XIX, 21 (1/2014), p. 29.
[33] *Ibidem.*

field of information security assurance is not easy due to the large number of systems and various initiatives undertaken in this area. However, it should be clear that this cooperation is developing very quickly. It seems that depending on the specific sector its effects will be seen in the near future.

Another important aspect of this case is education. All the time insufficient number of computer users are unaware that their computers may be targeted by teenage hacker or be used as a remote weapons by terrorists. Conducting awareness, but lacking the alarming tone of the educational campaign would certainly help improve safety in this area.

REFERENCES

[1] Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Wydawnictwo Wyższej Szkoły Cła i Logistyki, Warszawa 2011.

[2] Catelan N., Cimamonti S., Perrier J.B., *La luttecontre le terrorismedans le droit et la jurisprudence de l`Unioneuropeenne*, Press Universitaires, Marsylia 2014.

[3] Denning D., *Is Cyber Terror Next?*, www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc (14.05.2016).

[4] Gienas K., *Systemy Digital Rights Management w świetle prawa autorskiego*, Wolters Kluwer, Warszawa 2008.

[5] Gniadek A., *Cyberprzestępczość i cyberterroryzm – zjawiska szczególnie niebezpieczne* [w:] *Cyberterroryzm. Nowe wyzwania XXI wieku*, red. T. Jemioło, J. Kisielnicki, K. Rajchel, Wyd. WSIZIA, WSPOL, WSO AON, Warszawa 2009.

[6] Gryz J. (red.), *Zarys teorii bezpieczeństwa państwa*, Warszawa 2016.

[7] Indecki K., *Prawo karne wobec terroryzmu i aktu terrorystycznego*, Łódź 1998.

[8] Janowska A., *Cyberterroryzm – rzeczywistość czy fikcja?* [w:] *Społeczeństwo informacyjne. Wizja czy rzeczywistość?* v. I, Wyd. AGH, Kraków 2004.

[9] Kosiński J., Waszczuk A., *Cyberterroryzm a cyberprzestępczość* [w:] *Współczesne zagrożenia bioterrorystyczne i cyberterrorystyczne a bezpieczeństwo narodowe Polski*, red. P. Bogdalski, Z. Nowakowski, T. Płusa, J. Rajchel, K. Rajchel, WSPol, WSIZiA, WSOSP, WIM, Warszawa 2013.

[10] Kruk A.M., *Bezpieczeństwo transferu informacji w XXI wieku w świetle bezpieczeństwa państwa i organizacji* [w:] S. Sulowski, M. Brzeziński (ed.), *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, Wyd. Elipsa, Warszawa 2009.

[11] Lakomy M., *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*, „Stosunki Międzynarodowe" Vol. 42/2010.

[12] Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wyd. Adam Marszałek, Toruń 2006.

[13] Madej M., *Zagrożenie asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, PISM, Warszawa 2007.

[14] Oleksiewicz I., *Challenges of EU security on the example of cyberrorism policy*, "Journal of International Trade Law of Policy" (1/2015).

[15] Oleksiewicz I., *Ochrona praw jednostki a problem cyberterroryzmu*, HSS, Vol. XIX, 21 (1/2014).

[16] Polit M., *Cyberterrorism- Fact or Fancy?*, www.cs.georgetown.edu/~denning/infosec/pollitt.html (14.05.2012).

[17] Radoniewicz F., *Postanowienia decyzji ramowej Rady w sprawie ataków na systemy informatyczne a ujęcie cyberprzestępstw w kodeksie karnym*, „Ius Novum" No. 1/2009.
[18] Sakowicz A., *Prawnokarne gwarancje prywatności*, Zakamycze 2006.
[19] Schmitt M.N. (ed.), *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2015.
[20] Schreier F., *On Cyberwarfare*, „DCAF Horizon 2015 Working Paper", Vol. 7
[21] Siwicki M., *Cyberprzestępczość*, Wydawnictwo C.H. Beck, Warszawa 2013.
[22] Snyder R., *Hating America: Bin Laden as a civilizational revolutionary*, "Review of Politics" No. 4/2003.
[23] Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem*, LexisNexis, Warszawa 2010, p. 17.
[24] *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, red. M.N. Schmitt, Cambridge University Press, 2013.
[25] Zgorzały R., *Przestępstwo o charakterze terrorystycznym w polskim prawie karnym*, „Prokuratura i Prawo" No. 7–8/2007.
[26] The Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, drawn up in Lisbon on13 December 2007 (Journal of Laws of 2009, No. 203, item. 1569).
[27] Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence (JOLEU L 196 on 02.08.2003.)
[28] Council Framework Decision2005/222/JHA of 24 February 2005 on attacks against information systems (JOL EU L, No. 69, dated 16 March 2005).
[29] Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence Warrant (JOLEU L 350 on 30.12.2008).
[30] Council Decision 2009/426 /JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (JOL L 138, 4.06.2009).
[31] Directive of the European Parliament and of the Council 2011/93/EU of 13 December 2011 on combating the sexual abuse, sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/ JHA(JOL EU.L No.335 of December 17, 2011).
[32] Directive of the European Parliament and of the Council 2013/40/EU of 12 August 2013onattacks against information systems and replacing Council Framework Decision2005/222/JHA (JOL EUL 218 of 14 August 2013).
[33] Directive 2014/41/EU of the European Parliament and of the Council of 3rd April 2014 (JOLEU L 130 on 1.05.2014).
[34] European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 (CETS No.030).
[35] Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union (JOLEU C 197 on 12.07.2000.

PRAWNE ASPEKTY ZARZĄDZANIA POLITYKĄ ANTYCYBERTERRORYSTYCZNĄ UNII EUROPEJSKIEJ

Oprócz tradycyjnych zagrożeń dla informacji takich jak szpiegostwo lub przeciek tajemnic państwowych czy handlowych pojawiły się nowe zagrożenia, wśród których najbardziej

niebezpieczny jest cyberterroryzm. Prawidłowe funkcjonowanie społeczeństwa zależy dziś w dużym stopniu od właściwego zarządzania nowoczesnymi technikami i technologiami informatycznymi. Komputery i sieci komputerowe powszechnie stosowane są w gospodarce, administracji, jak również w codziennym użytku gospodarstw domowych. Biorąc pod uwagę problemy związane z cyberterroryzmem, a w szczególności analizy przepisów mających na celu zapewnienie bezpieczeństwo systemów informatycznych państw, to zagadnienie powinno być również uznane jako wymagające wnikliwej analizy badawczej.
W związku z tym niniejszy artykuł jest próbą wyjaśnienia, czym różni się cyberterroryzm od cyberprzestępstwa i jak należy rozumieć cyberbezpieczeństwo w dzisiejszych czasach. Podjęto próbę scharakteryzowania determinantów tego zjawiska i analizy analizę najnowszych rozwiązań prawnych w zakresie zarządzania polityką zwalczania cyberterroryzmu, jak i cyberprzestępczości w UE. Konstrukcja współczesnego modelu społeczeństwa informacyjnego, którego niezaprzeczalnym katalizatorem są technologie stosowane podczas komunikacji elektronicznej, przybierającej w wyniku konwergencji formę cyfrową, wyzwala potrzebę refleksji nad fenomenem informacji.
Podjęta analiza ma na celu przedstawienie wpływu unijnych instrumentów prawnych na zwalczanie samego zjawiska cyberprzestępczości. Ponadto starano się znaleźć odpowiedź na pytanie, czy obecne standardy prawne przyjęte w Unii Europejskiej w zakresie bezpieczeństwa są skutecznym narzędziem w zwalczaniu zagrożenia, jakim jest cyberterroryzm.

Słowa kluczowe: zarządzanie, cyberterroryzm, polityka, UE, prawo.

DOI: 10.7862/rz.2017.mmr.32

Tekst złożono w redakcji: lipiec 2017 r.
Przyjęto do druku: grudzień 2017 r.