Journal of International Trade, Logistics and Law, Vol. 1, Num. 1, 2015, 25-30

CHALLENGES OF EU SECURITY ON THE EXAMPLE OF CYBETERRORISM POLICY

Izabela Oleksiewicz, (PhD)

Technical University in Rzeszow, Poland

Abstract:

In addition to traditional threats to information as spying or leaking state secrets and business secrets appeared the new threats, among which the most dangerous is cyberterrorism. Taking into account the problems of cyber-terrorism, includes, in particular, the analysis of legislation aimed at ensuring the security of information systems of individual countries particular, this subject should be also recognized as requiring at the present time the insightful analysis.

Therefore, this publication is an attempt of characteristics the determinants of this phenomenon and analysis of the latest legal solutions in the fight against cyber terrorism within the European Union.

Moreover, it was made the attempt to find an answer to the question whether the current legal solutions of the European Union in the area of security are an effective tool in the fight against cyberterrorism.

Keywords:

Cyberterrorism; Policy; EU; Challenges

1. The Notion of Cybeterrorism

The definition of cyberterrorism had also given M. Pollite defining it as a deliberate, politically motivated attacks carried out by non-state groups or clandestine agents against information, computer systems, software, and data at the result of what the people not participating in the fighting experience the violence.(Polit, Cyberterrorism- Fact or Fancy?)

The term "cyberterrorism" appeared for the first time in 1979 in Sweden in the report showing 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 or result in considerable damage. In the 80s of the twentieth century this term was used in the American special services, pointing to the possibility of carrying out electronic attacks by the enemies of the United States. In 1998, at the Headquarters of the FBI created the National Infrastructure Protection Center (NIPC), whose task is to coordinate the collection of information about the threats, 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 activity is associated not only with the hostile use of IT and the action in the virtual sphere, but is also characterized by all constitutive elements for the terrorist activity (Denning, Is Cyber Terror Next?).. This term refers to the unlawful attacks and threats against computers, networks and the information held in them in the aim is to intimidate or coerce the government or its 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 property, or at least cause 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 intimidating or coercing the government and people of far-reaching political and social objectives in the broad sense of the word (Liedel, 2006, 36). This concept is the object of greater interest for at least of 80 s. of the twentieth century, and the speculations on

this subject have intensified after the attacks of 11 September 2001 in the USA. As a typical threats are indicated the traffic control systems, the bank infrastructure, the energy supply systems and water as well as personal database systems, and government institutions (Pomykała, 2009, 112-113)

The abovementioned definitions show that cyberterrorism is understood in the world in two ways. According to the first concept, the terrorism and cyberterrorism is distinguished only by the use of information technology to carry out the coup, while the second one 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 connecting of both approaches (Suchorzewska A, 2010).

Cybercrime is defined as a form of use of telecommunications networks, computer networks, Internet aimed breach of any good protected by law (Białoskórski, 2009)(Jemioły, 2009)(Kosiński, 2013). Cybercrime differs from the classic crime primarily operating in an environment related to computer technology and the use of computer networks to commit crimes (Siwicki, 2013). Its distinguishing feature is, however, not to protect any one of the common good (Siwicki, 2013). 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, too, and these negatively received. Increasingly frequently speaks of cyberspace as a new social space, which reflected the same problems as in the real world. Cybercrime is therefore a modern variant of crime, exploiting the possibilities of digital technology and the environment of computer networks.

This makes that protection against the threats posed by cybercrime is extremely difficult and requires taking a number of projects including challenging multi-faceted and broad international cooperation. The effectiveness of this protection 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. Thanks to these general rules require implementation into national law of the country, becoming the basis for institutional and functional system of instruments to fight cybercrime. The creation of an effective system to counter cybercrime is not easy, 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 law or EU into domestic law.

2. 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 motif of various terrorist groups. Cultural factor can also be a kind of barrier to mutual understanding of the objectives and intentions, the consequence must not be a terrorist attack in the traditional sense. The source of aggravating these tensions may be the fact that the cultural and civilizational diversities are often used as a bargaining chip in the event of a conflict, when in fact the sources of the real reasons for their rivalry are quite different (Snyder, 2003).

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

The processes of globalization, especially affecting the socio-economic sphere, create new security risks. It also has the importance of the fact that part of the crisis-phenomena takes place outside its territory. They directly impact 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 state1.

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

With the immateriality of cyberspace other characteristics are related. First of all, the network is global2. 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. Lack of not only strategic intelligence, but also, in many cases, the possibility of identification of the person responsible for the attack computer. This is, contrary to appearances, the problem of fundamental importance. Identification of the subject responsible for the break-in is in fact essential for the preparation of an appropriate policy response, judicial or military one.

Another important feature of cyberspace are relatively low operating costs there. The development of conventional military capabilities is 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 environment, in this perspective, are almost free3. The use of cyberspace helped by the fact that, as demonstrated operation in 2007 in Orchard the measures of this type can sometimes replace or supplement conventional military operations (Lakomy, 2010). Cyberspace and speed attacks make conducting defense activities difficult. At the same time as indicated above, the offensive actions are relatively cheap and easy to carry. This feature of cyberspace is more pronounced, as there is the greater dependence of societies on its application. 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 it a technologically advanced body which is much more sensitive to ICT attacks. In addition, as noted by Fred Schreier (Schreier, 2015), 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 on the defensive.

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 disinformation4.

3. New legislative changes in the counter cyberterrorism policy of the European Union

The latest Directive 2014/41/EU of the European Parliament and of the Council of 3rd April 2014(JOL EU L 130 on 1.05.2014). concerning the European Investigation Order (EIO) in criminal matters art. 1 paragraph 1 of the directive defines the broader concept of EIO than that which was contained in the Framework Decision

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

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

[3] 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. However they do not involve the major costs in terms of budget (the case of the Stuxnet virus).

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

2008/978/JHA. In the current wording it means a judicial decision issued or approved by a judicial authority5 "the issuing State"6 to call "the executing State"7 to carry out one or several specific investigative order to obtain evidence.

The directive shall apply from 21st May 2014 to 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 the execution in the European Union of orders freezing property or evidence and the Framework Decision 2008/978 / JHA on the European evidence Warrant (JOL EU L 350, 30.12.2008).

The EIO is like the EAW of 2008 another instrument based on the principle of mutual recognition. Thus, facilitating 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 an useless instrument because it requires certainty as to the presence of evidence in the requested State (*Catelan*, *Cimamonti*, *Perrier,* ,2014, 135) In connection with this new instrument or EIO, which was created, it covers almost all investigative and does not have this requirement. These instruments are crucial in the fight against the use of the Internet for terrorist purposes, because they allow rapid international cooperation.

The EIO mechanism was created to enable the courts, prosecutors and other investigative authorities for a direct transmission of requests for 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 it has seen European orders in the same way as those issued by national authorities.

According to article 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 Article 13 paragraph 8 of the Convention and Article 1, section 8 of the Framework Decision 2002/465 / JHA (JOL L 138, 4.6.2009).

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

[5] 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.
[6] This means the Member State in which the EIO is issued (Art. 2 paragraph 1 item a).
[7] This means the EIO executing Member State in which you want to perform a particular investigative measure (Art. 2 paragraph. 1 item b).

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 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.

4. Conclusion

The fact is that modern information systems which form part of the critical infrastructure of the country require a much more solid protection than it seemed a few years ago. The effect of rapid technological development has become a strong dependence of the economy on IT systems. They control nowadays 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.

The need for security seems to be a self-evident truth. Some companies are aware of this fact, others unfortunately not. Certainly protection systems can be improved through the introduction of new legislation providing good practices in the area of security. However we must remember to set new rules balance the need for security with the right to privacy (Oleksiewicz, HSS, vol. XIX, 21 (1/2014), 113-130).

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 develop its potential in this field. One can understand not only employed professionals and their infrastructures, but also the techniques and tools used in ICT attacks. Rightly it recognized that in its present form Cyberspace can be effectively applied to meet specific interests in the international environment.

Another regulation EIO introduced is 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 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

Bialoskórski, R. (2011), "Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki" Wydawnictwo Wyższej Szkoły Cła i Logistyki, Warszawa.

Catelan N., Cimamonti S.,. Perrier J.B. (2014), La lutte contre le terrorisme dans le droit et la jurisprudence de l`Union europeenne, Press Universitaires, Marsylia.

Denning D. "Is Cyber Terror Next?" avaible at: http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc. (accessed 14 May 2009).

Gniadek A.(2009), Cyberprzestępczość i cyberterroryzm – zjawiska szczególnie niebezpieczne, [in:] Cyberterroryzm. Nowe wyzwania XXI wieku pod red. T. Jemioły, J. Kisielnickiego, K. Rajchela, Wyd. WSIZIA, WSPOL, WSO AON, Warszawa.
Janowska A.(2004), Cyberterroryzm - rzeczywistość czy fikcja? [in:] Społeczeństwo informacyjne. Wizja czy rzeczywistość? v. I, Wyd. AGH, Kraków.
Kosiński J., Waszczuk A.(2013), Cyberterroryzm a cyberprzestępczość, [in:], 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.
Lakomy M.(2010), Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku, „Stosunki Międzynarodowe"vol. 42.
Liedel K.(2006), Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego, Wyd. Adam Marszałek, Toruń.
Madej M.(2007), Zagrożenie asymetryczne bezpieczeństwa państw obszaru transatlantyckiego, PISM, Warszawa.
Oleksiewicz I.(2014), Ochrona praw jednostki a problem cyberterroryzmu, HSS, vol. XIX, 21.
Polit M., Cyberterrorism- Fact or Fancy? , avaible at: http://www.cs.georgetown.edu/~denning/infosec/pollitt.html (accessed 14 May 2009).
Pomykała M., Cyberterroryzm [in:] Bezpieczeństwo i zagrożenia współczesnego świata, red A. Olak, I. Oleksiewicz.
Schreier F.(2015), On Cyberwarfare, „DCAF Horizon 2015 Working Paper", t. 7
Siwicki M.(2013), Cyberprzestępczość, Wydawnictwo C.H.Beck, Warszawa.
Snyder R. (2003), Hating America: Bin Laden as a civilizational revolutionary, "Review of Politics" no: 4
Suchorzewska A.(2010), Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem, LexisNexis, Warszawa.
JOL EU L 130 on 1.05.2014.
JOL EU L 350, 30.12.2008.
JOL L 138, 4.6.2009.