Teka Kom. Politol. Stos. Międzynar. – OL PAN, 2016, 11/3, 135–146

DILEMMAS AND CHALLENGES FOR EU ANTI-CYBERTERRORISM POLICY: THE EXAMPLE OF THE UNITED KINGDOM

Izabela Oleksiewicz
Politechnika Rzeszowska
Zakład Nauki o Bezpieczeństwie
e-mail: oleiza@interia.pl

Abstract: In the modern world the expansion of the semantic field of security takes place, which is the reason for the existence of a number of risks, with a very wide dimension. In addition to traditional natural hazards and existing threats to civilization, there is a new one that is closely related to the implementation of modern technologies, information systems, and communication systems. They are a sign of the times and an inevitable consequence of progress. At the same time society (especially informed civil society) requires more and more of their country, demanding ever higher levels of security and protection to enable its further development. Providing such protection requires considerable strengths and resources, and the intersectoral cooperation of public and private subjects. Developing international contacts and extensive cooperation in this dimension is necessary, but existing forms of security protection are limited to the territory of one state and cannot fulfill these tasks. The fight against terrorism is also a question of access to information about people traveling regularly or prolonging their stay in other states.
In the face of these processes we should look for new solutions and undertake such activity, with a scale corresponding to the scale of risk. The cooperation of various entities – understood as combining expertise, manpower and resources – while engaging modern technology, seems to be most appropriate.

Key words: terrorism, cyberterrorism, anti-cyberterrorism policy, European Union, United Kingdom

1. THE GENESIS AND NOTION OF CYBERTERRORISM

Cyber terrorism has become a fashionable concept, but few people know what it really means. Many people believe that this is only a theoretical concept, an action that probably will never happen in reality. But no one knows what the future will hold. A few years ago, only a few people considered the likely agenda that occurred on 11 September 2001 in New York. It seems that one can fully agree with the words of D. Verton that an unforeseeable terrorist attack is simply

an attack that has never been. Therefore, the creation of adequate to insure information systems information systems, primarily through the creation of effective regulation in this area it seems to be extremely important and up-to-date.

One of the first definitions of computer crime, proposed in 1973 by R. von Zur-Miihlena, was that computer crime is "any criminal activity in which the computer is either a tool or object coup".[1] By contrast, H. J. Schneider term defines it as "a crime at which devices for electronic data processing are used as a tool for crime or for which such devices are the subject of assassination".[2]

The definition of cyberterrorism was given M. Pollite in 1997, defining it as a deliberate, politically motivated attack carried out by non-state groups or clandestine agents against information, computer systems, software, and data with the result that people not participating in the fighting experience the violence. (Polit, *Cyberterrorism- Fact or Fancy?*)

The term "cyberterrorism" first appeared in a 1979 Swedish 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, the intimidation of governments and societies to exert psychological pressure, bringing life-threatening dangers or resulting in considerable damage. In the 1980s, 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. The FBI created the National Infrastructure Protection Center (NIPC) 1998; its 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 it is associated not only with the hostile use of IT and action in the virtual sphere, but is also characterized by all the elements of 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 with the aim to intimidate or coerce the government or its people in order to achieve certain political or social benefits. In addition, in order to characterize an attack as a cyberterrorism attack, it should result in 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 intimidate or coerce the government and people in order to realize far-reaching political and social objectives (Liedel, 2006, 36). This concept is the object of greater interest since at least the 1980s, and speculation on this subject intensified after the 11 September 2001 attacks.

[1] M. Siwicki, *Materiały szkoleniowe*, Prokuratura i Praw o nr 7–8/2012, p. 242; Patrz też: R. v on Zur-Muhlen, *Computerkriminalitat. Gefahren und Abwehr*, Neuwied, Berlin 1973.

[2] M. Siwicki, *Materiały szkoleniowe…,* p. 243.

Typical targets are traffic control systems, the bank infrastructure, 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 two ways. According to the first concept, terrorism and cyberterrorism are distinguished only by the use of information technology to carry out the attack, while the second 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.[3]

Cybercrime is defined as a form of use of telecommunications networks, computer networks, or the Internet aimed at breaching of any good protected by law.[4] Cybercrime differs from classic crime primarily operating in an environment related to computer technology and the use of computer networks to commit crimes. Its distinguishing feature is, however, not to protect any one of the common goods (Siwicki, 2013, 20–21). Today, almost every illegal activity is reflected on the Internet. The global nature of the Internet allows for extremely fast communication and the transfer of most forms of human activity to the network, too, and these negatively received. Increasingly frequently, one speaks of cyberspace as a new social space, reflecting 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 protection against the threats posed by cybercrime extremely difficult and requires taking on a number of projects requiring challenging, multi-faceted, and broad international cooperation. The effectiveness of this cooperation requires individual countries to establish a common policy against cybercrime and its concretization, specifying priorities and uniform principles of joint action. These general rules require implementation into the national law of the country, becoming the basis for an institutional and functional system of instruments to fight cybercrime. The creation of an effective system to combat cybercrime is not easy, and requires a thorough analysis of the phenomenon in the long term. The creation of such a system may encounter numerous problems in adapting the general guidelines of international or EU law into domestic law.

---

[3] See also: A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem*, LexisNexis, Warszawa 2010, p. 17.

[4] View R. Białoskórski, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Wydawnictwo Wyższej Szkoły Cła i Logistyki, Warszawa 2011, p.63 and next.; A. Gniadek, *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 2009, p. 222 and next.; J. Kosiński, A. Waszczuk, *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 2013, p. 333.

2. THE EU INTERNAL SECURITY DETERMINANTS

Religious, demographic, social and ideological issues – apart from military and economic challenges – have become the main factors of the crisis in Europe today. Undoubtedly, cultural differences, and especially religion are the main motif of various terrorist groups. Cultural factors can also be a kind of barrier to mutual understanding of objectives and intentions, but may not result in a traditional terrorist attack. Aggravating these tensions might be the fact that cultural and civilizational differences are often used as a bargaining chip in the event of a conflict, when in fact the source of the real reasons for their rivalry are quite different.[5]

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

The processes of globalization, especially affecting the socio-economic sphere, create new security risks. Some of the crisis-phenomena take place outside of the state's territory. These directly impact the internal situation of European countries and the European community. Large sections of communities want to maintain security of employment and an adequate number of jobs, and believe that the appropriate level of social security and cultural identity should be a priority task of the state.[6]

To find an answer to the question of what a cyber-war actually is, it is first 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 as 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.

Other characteristics are related to the immateriality of cyberspace. First of all, the network is global.[7] As a consequence, the limitations of a physical character do not apply here. It is relatively easy to hide the real identity of the perpetrators of ICT incidents due to a lack of not only strategic intelligence, but also, in many cases, the possibility of identification of the person responsible for

[5] Compare: R. Snyder, *Hating America: Bin Laden as a civilizational revolutionary*, "Review of Politics" no. 4/2003, pp. 325–349; M. Madej, *Zagrożenie…,* p. 86.

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

[7] 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.

the attack computer. This is, contrary to appearances, a 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.

Another important feature of cyberspace is the 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. In contrast, the tools that can be used to attack the ICT environment are almost free.[8] The use of cyberspace can sometimes replace or supplement conventional military operations.[9] Cyberspace and speed attacks make conducting defense activities difficult. At the same time as indicated above, offensive actions are relatively cheap and easy to carry out. This feature of cyberspace is more pronounced, as there is greater dependence of societies on its application. A 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 this creates a technologically advanced body that is much more sensitive to ICT attacks. In addition, as noted by Fred Schreier[10], 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.

The last group of reasons why cyberspace is of growing interest in countries is 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 disinformation.[11]

3. LEGAL ASPECTS OF EU ANTI-CYBERTERRORISM POLICY

The entry into force of the Treaty of Lisbon in 2007 brought qualitative change in developing tools to combat cyber-crime (Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, OJC 115, vol. 51, 9.05.2008), under which criminal law became a separate, though specific, policy of cooperation (M. Siwicki, *Cyberprzestępczość*…, p. 41). Opening the route to harmonization of substantive and procedural criminal law,

[8] 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).

[9] Compare. M. Lakomy, *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*, „Stosunki Międzynarodowe"vol. 42/2010, p. 56.

[10] View more: F. Schreier, *On Cyberwarfare*, „DCAF Horizon 2015 Working Paper", t. 7, p. 11.

[11] An interesting manifestation of such measures were 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.

Art 83 paragraph 1 TFEU laid down the principle that under EU law minimum rules concerning the definition of criminal offenses and sanctions in the areas of particularly serious crime with a cross-border dimension can be established. It clearly indicates that computer crime is included.

The latest directive (2014/41/EU of the European Parliament and of the Council of 3 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 a broader concept of EIO than was contained in the Framework Decision 2008/978/JHA. In the current wording, a judicial decision issued or approved by a judicial authority[12] in „the issuing State"[13] calls upon „the executing State"[14] to carry out one or several specific investigative orders to obtain evidence.

The directive applies from 21 May 2014 to 22 May 2017. Member States shall take the necessary measures to meet its requirements. It replaces the existing rules 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 ratified by Poland. As well as the Council Framework Decision 2003/577/JHA the executive in the European Union 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 of 2008 is often rated as a useless instrument, because it requires certainty as to the presence of evidence in the requested State (Catelan**,** Cimamonti**,** Perrier, 2014, 135) In contrast, the newly-created instrument or EIO covers almost all investigations 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 to use direct transmission by videoconference of requests for specific proof, to secure and search the property or hold a hearing. The judicial authority of the country, to which EIO is 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.

[12] 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.

[13] This means the Member State in which the EIO is issued (Art. 2 paragraph 1 item a).

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

According to article 3, the objective range of the EIO governing each investigative action beyond creation of a joint investigation team and the gathering of evidence by the team is 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, an EIO directive may be issued:

a) with respect to criminal proceedings initiated by a judicial authority or that may be brought before a judicial authority in the case of an offense under the law of the issuing State;
b) in proceedings brought by the authorities with respect to 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 with respect to acts 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.

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) the investigative measure(s) indicated in the EIO are permissible under the same conditions in a similar national case management to carry out

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 of the so-called EIO as to why they were taken. After such consultation, the issuing authority may also decide to withdraw the EIO.

4. LEGAL FRAMEWORK FOR CYBERTERRORISM IN UK NATIONAL POLICY

A major challenge for Europe was the increased travel by European citizens – mostly young men – to and from Syria to join forces opposing the Asad regime. Many of them ended up in the ranks of violent extremist groups such as the al-Nusrah Front or the Islamic State of Iraq and the Levant (ISIL). These "foreign fighters" sparked increasing concerns and actions by European countries worried about the growing number of citizens traveling to the battlefield and possibly

returning radicalized. European governments, in particular the EU and several member states affected by this phenomenon, took action to assess the problem and to devise an array of responses to discourage their citizens from going to Syria. These efforts ranged from new administrative procedures to prevent travel to Syria, steps to counter recruitment and facilitation efforts, and programs to investigate and/or reintegrate persons returning from conflict zones. Governments in EU candidate states and aspirants in the Western Balkans were also committed to responding effectively to the foreign fighter problem, and sought assistance from the United States, the EU, and others to fill gaps in their capacity to do so. European governments also worked with the United States and other international partners in various fora, including the Global Counterterrorism Forum, to respond to the foreign fighter problem and strengthen general counterterrorism cooperation

The UK launched its Prevent strategy to counter radicalization in 2007. Prevent is part of the government's overall national counterterrorism strategy, CONTEST. In 2011, Prevent was revised to correct several perceived problems. There had been complaints from members of Muslim organizations that UK government interaction with their communities was focused solely on security concerns. As a result, the UK divided the responsibilities for various strands of Prevent among different government organizations. The Department of Communities and Local Government took over responsibility for "integration" work, designed to ensure that Muslim communities received all the government services to which they were entitled and that immigrants were given assistance to integrate into British society. The Home Office focused on countering the ideology of violent extremism, including the identification of at-risk youth and their referral to counseling programs. The revised strategy called for a much more focused effort to target those most at risk of radicalization. Finally, the government decided that organizations that hold "extremist views," even those that are non-violent, will not be eligible to receive government funding or participate in Prevent programs (See I. Oleksiewcz, *Ochrona praw jednostki a problem cyberterroryzmu*, HSS, vol. XIX, 21 (1/2014), p. 113–130).[15]

Following the May 2013 murder of soldier Lee Rigby, the UK government launched a task force to determine whether the government was doing all it could to confront violent extremism and radicalization to violence. The task force suggested further actions that could be taken to disrupt violent extremists, promote integration, and prevent radicalization, particularly in schools and prisons (I. Oleksiewicz, *Polityka…,* p. 368).[16]

Under the Northern Ireland constitutional settlement, the UK government is responsible for Northern Ireland's national security and is covered by CONTEST. Following the devolution of policing and justice matters in April 2010,

[15] Compare https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf (12.11.2015)

[16] Compare http://www.refworld.org/docid/536229ab8.html (12.11.2015).

the Northern Ireland Minister of Justice is responsible for policing and criminal justice policy matters.

As a society emerging from conflict, Northern Ireland retains many divisions and grievances, and is home to a significant number of ex-prisoners. At the grassroots level, much of the work countering violent extremism is implemented by local community organizations. The majority of youth organizations, community safety projects, restorative justice programs, and neighborhood renewal programs have partnership working arrangements with the Police Service of Northern Ireland; some of these programs are directed and staffed by former combatants. Many NGOs, including some that work on a cross-border/all-Ireland basis, are engaged in efforts to prevent young people from becoming involved in "ordinary" crime, gang membership, and sectarianism. One such program, PEACE III (2007–2013), is a distinctive EU structural funds program with an emphasis on youth and unemployment, reinforcing progress toward a peaceful and stable society, and promoting reconciliation. The program has a total budget of approximately US $500 million, and covers Northern Ireland and the border region of Ireland.[17]

In 2013, the UK continued to play a leading role in countering international terrorism. The UK government continued to implement its updated counterterrorism strategy, CONTEST, which was released in 2011.[18] This update of CONTEST set out the UK's strategic framework for countering the terrorist threat at home and abroad for 2011–2015.[19] In 2013, the conflict in Syria proved to be a galvanizing force for UK-based Muslim individuals and organizations. The threat of European fighters traveling to Syria and then returning home radicalized and dangerous drew significant attention and resources.

Northern Ireland continued to experience a persistent level of security incidents, including attempted bombings, violent protests, and the placement of hoax explosive devices. Many of the devices were relatively crude but occasionally viable. Police Service of Northern Ireland (PSNI) officials reported an upsurge in dissident republican (Irish nationalist) attacks in 2013, as evidenced by letter

[17] http://www.state.gov/j/ct/rls/crt/2013/224822.htm (12.11.2015)

[18] *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world*, November 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (12.11.2015)

[19] The United Kingdom monitors the Internet in the context of its strategy to reduce the risk from terrorism by tackling the radicalisation of individuals, disrupting terrorists and their operations, reducing the vulnerability of the UK and UK interests overseas and preparing for the consequences of a terrorist attack. Internet monitoring is particularly relevant with respect to the first two of these objectives. This activity, and all other activities to prevent criminal and other types of cybercrime, are carried out under a range of legal provisions notably the Regulation of Investigatory Powers Act 2000 and adhering to relevant EU legislation and conventions. The United Kingdom takes a flexible intelligence-led approach which leads to specific monitoring of themes, groups or websites according to national requirements and priorities. See more: http://www.coe.int/t/dlapil/codexter/country_profiles.asp(12.11.2015).

bombs, under-car booby traps, blast bombs, and hijackings. While security forces and facilities continued to be the primary targets of violence, a few attempts were aimed at political officials and commercial centers within Belfast's city center (more I. Oleksiewicz, *Polityka…,* p. 374).[20]

In October 2012, the British Security Service downgraded the threat to Great Britain from dissident Irish republicans from "substantial" to "moderate". The decrease shows the authorities regard an attack on London and other British cities from such groups as possible, but not likely. Previously it was deemed a strong possibility. The threat level in Northern Ireland has not changed. It remained „severe" with an attack still highly likely. On its website, MI5 said: „The threat level for Northern Ireland-related terrorism is separate from that for international terrorism. It is also set separately for Northern Ireland and Great Britain."[21]

It is UK practice to criminalise specific actions rather than the medium through which the actions are committed. There are therefore a number of terrorist-related actions that could take place in cyberspace that are unlawful in the UK, such as the dissemination of terrorist publications or the encouragement of terrorism, but the illegality of these is not limited to their taking place in cyberspace.[22]

UK laws allow the government to investigate and prosecute terrorists using a variety of tools. On 25 April 2013, a key piece of security legislation, the Justice and Security Act, was passed into law. The bill closed a significant legal loophole in the government's ability to protect classified information; allowed "closed material proceedings" in civil courts, thus enabling the government's use of classified information to defend itself in civil cases; and strengthened parliamentary oversight of the intelligence community (see I. Oleksiewicz, *Polityka…,* p. 356).

The UK has a highly capable network of agencies involved in counterterrorism efforts. The Metropolitan (Met) police lead the UK's national counterterrorism law enforcement effort. The Met police work closely with local police, MI5, and other agencies in terrorism investigation, prevention, and prosecution. On 7 October 2013, the National Crime Agency (NCA) was launched and absorbed its predecessor, the Serious Organized Crime Agency (SOCA). While the NCA is not the lead counterterrorism agency, its organized crime, cybercrime, and border policing remit involved it in some counterterrorism issues (I. Oleksiewicz, *Polityka…,* p. 372).[23]

The UK has issued machine readable passports with an imbedded electronic chip since 2006. UK travel documents and visas contain a number of security features to prevent tampering and fraud. The UK has advanced biometric screening capabilities at some points of entry, but at others there is no screening at all. The UK has no statutory ability to collect advance passenger name records (PNR). It

[20] Compare http://www.ecoi.net/local_link/275238/391151_en.html (12.11.2015).

[21] *Ibidem*.

[22] See also https://www.coe.int/t/dlapil/codexter/Source/cyberterrorism/United%20Kingdom.pdf (12.11.2015).

[23] See also http://www.refworld.org/docid/5587c73830.html (5.12.2015).

is against EU regulations for the UK to collect PNR information on commercial flights originating from within the EU.

The UK is also a member of the Financial Action Task Force (FATF) and an active participant in FATF-style regional bodies to meet evolving money laundering and terrorist financing threats, and has a wide range of anti-money laundering and counterterrorist finance laws. The UK has been a leader on pointing out the dangers of paying kidnappers' ransom payments and developing the linkages of ransom payments to increased financial support for terrorist organizations and further kidnappings.[24]

5. CONCLUSIONS

To sum up, in order to run counter-terrorism policy effectively, it must combine elements of prevention whose aim is preventing terrorism by taking appropriate measures, and punishment, involving the punishment of terrorists, accomplices, instigators and helpers of such crimes. The strength of a good criminal justice system lies in how to put boundaries between prevention and punishment.

A condition limiting the impact of security threats is presented reaction to their source. A requirement is the abandonment of a policy popular among the European political establishment – the policy of „self-ease", i.e., assuming that the risks themselves are gone--is needed. A significant part of the ongoing projects should be directed to regions of political and economic instability.

The fight against terrorism is just one of the special subjects of law and the criminal justice regime, specialized and adapted to the specific nature of terrorism. This applies in particular to punishing terrorist organizations and organized crime groups.

Police departments responsible for combating terrorism need to have access to information about people traveling regularly or prolonging their stay in countries known as areas of radicalization as well as information on the movements of units already identified as terrorist ones.

Combating terrorism through measures to facilitate an efficient reaction to a given crime can be assessed primarily in terms of their impact on general and specific prevention. On the one hand, we are dealing with a strong, ideologically-motivated perpetrators of terrorist acts who do not usually fear swift and harsh punishment. On the other hand, we need to deal with suicide terrorists. It follows that the measures already made in response to the act, particularly to its most tragic consequences, they will play a supporting role in the fight against this phenomenon. Therefore, the fight against terrorism must be based primarily on

[24] For further information on money laundering and financial crimes, see the *2014 International Narcotics Control Strategy Report (INCSR), Volume 2, Money Laundering and Financial Crimes*: http://www.state.gov/j/inl/rls/nrcrpt/index.htm (12.11.2015).

prevention, i.e. on operational activities conducted by specialized services and far-reaching socio-political programs. Thus, even the best instrument to punish the perpetrators of terrorist acts cannot be a leading weapon in the fight against this form of crime and will act as a complementary part of the whole system of measures.[25]

DYLEMATY I WYZWANIA DLA ANTY-CYBERTERRORYSTYCZNEJ POLITYKI UE – PRZYPADEK ZJEDNOCZONEGO KRÓLESTWA

Streszczenie: We współczesnym świecie następuje stałe rozszerzanie się zakresu znaczeniowego bezpieczeństwa, czego powodem jest istnienie wielu zagrożeń, mających bardzo szeroki wymiar. Obok tradycyjnych zagrożeń naturalnych i dotychczasowych zagrożeń o charakterze cywilizacyjnym pojawiają się wciąż nowe, które mają ścisły związek z wdrażaniem nowoczesnych technologii, systemów informatycznych, systemów komunikacji. Są one znakiem czasu i nieuchronną konsekwencją postępu. Jednocześnie społeczeństwo (zwłaszcza informacyjne społeczeństwo obywatelskie) wymaga coraz więcej od swojego państwa, żąda coraz wyższego poziomu zabezpieczenia i ochrony, umożliwiającego mu dalszy rozwój. Zapewnienie takiej ochrony wymaga zaangażowania znacznych sił i środków oraz międzysektorowej współpracy podmiotów publicznych i prywatnych. Rozwijanie kontaktów międzynarodowych i szeroko zakrojonej współpracy w tym wymiarze powoduje, że dotychczasowe formy ochrony bezpieczeństwa ograniczone do terytorium jednego państwa przestają spełniać swoje zadania.
Nie należy zapominać, że warunkiem ograniczania oddziaływania przedstawionych zagrożeń bezpieczeństwa jest reakcja na ich źródła. Walką z terroryzmem jest również kwestia dostępu do informacji o osobach podróżujących regularnie lub przedłużających pobyt w państwach.
W obliczu tych procesów należy poszukiwać nowych rozwiązań i podejmować takie działania, których skala będzie odpowiadała skali zagrożeń. Współpraca różnych podmiotów – rozumiana jako łączenie wiedzy, sił i środków – przy jednoczesnym zaangażowaniu nowoczesnych technologii, wydaje się być najodpowiedniejsza.

Słowa kluczowe: terroryzm, cyberterroryzm, anty-cyberterrorystyczna polityka, UE, Zjednoczone Królestwo

[25] K. Kuczyński, *Znaczenie ENA w zwalczaniu terroryzmu…*, s. 157.