CYBERTERRORISM AND THE PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURES. A SNAPSHOT OF THE CURRENT STATE OF CERTAIN REGULATORY ISSUES.

Szerzők:

Helyes Marcell (Drs.)
Nemzeti Közszolgálati Egyetem

Szerző e-mail címe:
marcell.helyes@gmail.com

Lektorok:

Haig Zsolt (Prof.Dr.)
Nemzeti Közszolgálati Egyetem

Mihók Sándor (dr.jur)
nyugalmazott jogtanácsos

…és további két anonim lektor

Absztrakt

KIBERTERRORIZMUS ÉS A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELME. HELYZETKÉP A SZABÁLYOZÁSI PROBLÉMÁK JELENLEGI HELYZETÉRŐL.

A nyugati államok évtizedek óta harcolnak a terrorizmus ellen, azonban egyes alapvető szabályozási kérdések a mai napig megválaszolatlanul maradtak. Következésképpen a konvencionális terrorizmushoz hasonlóan a terrorizmus legújabb formája, a kiberterrorizmus kapcsán is számos jogi bizonytalanság tapasztalható. A (kiber-)terrorizmust szabályozó nemzetközi egyezmények bonyolult és hiányos rendszere a kérdéskör csak bizonyos vonatkozásairól rendelkezik, továbbá alapvetően az államok felelősségi körébe helyezi a (kiber-)terrorizmus szabályozását anélkül, hogy egyes alapvető normák egységes rendszerét felállítaná. Jelen írásban a szerző a kiberterrorizmus nemzetközi és nemzeti jogi vonatkozásait tárgyalja kiemelve a kritikus információs infrastruktúrák védelmének különleges területét. Ugyancsak említésre kerül a kiberterrorizmus a nemzetközi humanitárius jog tükrében.

Kulcsszavak: kiberterrorizmus, kritikus információs infrasturktúrák, kiberbűnözés, kibertámadás, kibervédelem, terrorelhárítás

Diszciplinák: informatika, hadtudomány, jogtudomány

Abstract

Western states fight against terrorism for decades now, however, certain fundamental regulatory questions stay unanswered to this day. Consequently, with the newest form of terrorism, cyberterrorism, arise just as many legal uncertainties as with conventional terrorism.

The complicated and incomplete system of international treaties on (cyber-)terrorism only cover certain aspects of the issue, moreover they generally make the individual states responsible for regulating (cyber-)terrorism without defining a common system of basic rules. In this paper the author discusses cyberterrorism from an international and national legal perspective highlighting the specific area of critical information infrastructure protection. Furthermore the paper also takes into consideration cyberterrorism in the light of international humanitarian law.

Keywords: cyberterrorism, critical information infrastructures, cybercrime, cyber-attack, cyber-defense, counter-terrorism

Disciplines: information technology, military sciences, law

Helyes, Marcell (2021): Cyberterrorism and the protection of critical information infrastructures. A snapshot of the current state of certain regulatory issues.. *Lélektan és hadviselés – interdiszciplináris folyóirat*, III. évf. 2021/1. szám. 51-68. doi: 10.35404/LH.2021.1.51

Although part of the literature still argues that cyberterrorism is not a real threat (Cohen-Almagor, 2018), the author believes it not to be the case. To the contrary, the author considers it only a matter of time, until terrorist groups become regular perpetrators of cyber-attacks besides states and purely financially motivated cybercriminals. In cyberspace, acts of malicious intent can be carried out with very little funds, but on a large scale and often without the fear of identification. The information systems of critical infrastructures are facing one of the biggest cyberthreats coming from international terrorist organizations, therefore it is very important to ensure an effective and secure cyber defense system both on a technical and on a regulatory level.

It is clear that state authorities have a great interest in regulating cyber-related actions, however, numerous problems came to light in connection with the regulation of cyber-terrorism both on the level of international law, as well as on the level of national law.

In this article, the author presents considerations regarding the definition of (cyber-)terrorism and critical information infrastructures, as well as possible demarcations from other related areas of malicious cyber-activities. The author then presents cyber-terrorism in the system of international law stressing certain significant regulatory deficiencies and pressing questions. Lastly, the author discusses the regulatory framework of cyberterrorism in Hungary.

Cyberterrorism and critical information infrastructures

To discuss cyberterrorism, first, terrorism as well as international terrorism need to be defined. Unfortunately, to this day, there is no internationally accepted common definition on terrorism. There have been numerous attempts for finding the possible aspects of

classification, however, no result became part of international law yet. Clearly, defining what terrorism is, or what does not actually fall under the scope of terrorist activity is one of the most fundamental questions, and the lack of a common term leads to significant regulatory difficulties. Moreover, as discussed later, it makes impossible to create an international agreement specifically for the fight against international terrorism in its modern form.

However, despite the lack of an exact definition, it is still possible to make a distinction between terrorism, international terrorism and cyberterrorism. Terrorism is of national character, no cross-border actions take place in this case, hence the aim of a terroristic attack is to achieve a change on a national political level. Terrorism was dominant from the 19th century up until the 1960s, during the first two waves of terrorism (Martinez, 2016). Then the term international terrorism was created as a consequence of the new era of terrorism, also known as the third (revolutionary) wave of terrorism during the 1970s and it has since evolved into the fourth (religious) wave of terrorism (Martinez, 2016). International terrorism is not concentrated in one singular state but is connected to multiple states.

Based on the international and borderless character of cyberspace, or more precisely, since the state from which the cyberattack is launched (especially with a terrorist motive) often differ from the targeted state, cyber-terrorism must be categorized as a form of international terrorism. The main goals of cyberterrorism do not differ from the of the traditional international terrorism, only cyber-terrorism is enabled by information communication technologies and it takes place in cyberspace. Kovács and Illési defined for which purposes terrorist groups could possibly use information technology (Kovács & Illési, 2011):

- planning,
- communication,
- secret connections,
- organizing,
- recruitment,
- propaganda,
- fundraising,
- gaining data and information.

Two main group of actions of cyberterrorists can be identified (Shiryaev, 2013). On one hand, there are Internet based criminal actions that support the overall functioning of a terrorist group, such as fundraising, dissemination, secure communication and recruiting new members through propaganda (Pataki & Kelemen, 2014). On the other hand, there is a possibility of actual cyberattacks coming from terrorist groups with the intent of disrupting or destroying the information systems of (critical) infrastructures, or to steal valuable data from them (Mikac, Mamic, & Zutic, 2020).

It can be argued that cyberterrorism is the future of international terrorism, because the attacks are easily scalable, less risky and disproportionately cheap (Fidler, 2016), however, it needs to be stressed, that in the eye of the general public, cyberattacks happen behind-the-scenes, therefore it is hard to reach one of the main goals of terrorist groups by cyber means, namely, to cause fear. Nevertheless, the author of this paper argues, that

by attacking the critical information infrastructures of a state, this goal would be very well reached. For example, a disruption in service in the financial, energy, or telecommunication sector, or a combination of them, would rapidly lead to a general distress, and after a short while to panic and terror in any western state. On a different note, it has to be mentioned that, because of the invisible nature of cyber-attacks, in order to avoid public distress, the state that has been attacked would most probably deny terrorist involvement, and would officially regard the disruption in service as a pure malfunction.

It must be noted also that in certain cases a cyberattack is only the first step in a line of actions and not the attack itself causes the destruction, but it is strictly necessary for achieving the goal. For example, a cyber-attack against the information infrastructure of a nuclear reactor can lead to the dispersal of radioactive material.

Critical information infrastructures are critical infrastructures themselves or are integral part of other critical infrastructures and serve their functioning. Even though, they are not connected to the Internet for security reasons, their vulnerability still possibly imposes a major risk for every state's national security. It is not without example, that an attacker manages to get into the information systems of critical infrastructures and causes malfunction or an outage in the performance (Tóth, 2016).

Critical information infrastructures are one of the most probable targets of cyber-terrorists, as well as opposing states, because the short-term and long-term effects of a successful cyberattack on just one critical information infrastructure can be enormous. Additionally, it may possibly lead to the failure of service of multiple critical infrastructures deriving from the general rule of inter-dependency among critical infrastructures. Wall argues that the main characteristic of cyberterrorism, which in fact makes it differ from hacktivism mainly is that cyberterrorist attacks are carried out against critical infrastructures (Dornfeld, 2019).

Differentiating cyberterrorism from other acts of malicious intent in cyberspace

Firstly, in the context of defining cyber-terrorism, the question always arises, where can the line be drawn between cyberterrorism and cybercrime, moreover, whether there is a strict line at all. The literature points out that the methods of cyberterrorism and cyber-crime overlap to a great extent. From targeted and non-targeted cyberattacks to crimes that already existed, but are now enabled through today's information technology, such as money laundering for example, all of them might be carried out by cybercriminals as well as cyberterrorists. The main difference lays in the motive of the perpetrator. Cybercriminals mostly act because of the financial benefit of cybercrimes, or in a few cases just for the sake of it, whereas for terrorist groups, there is always a political, ideological, or religious agenda behind their cyberactivity.

Dornfeld emphasizes, that it is unreasonable and disadvantageous to draw a hard line between cyberterrorism and cybercrime, and it can only be done theoretically anyways,

because in most cases the attacker is unidentifiable, the methods and tools are in both cases often the same, and the motives are in reality often unclear (Dornfeld, 2019). Since with a cyberterrorist attack it is hard to get across the political, ideological, or religious agenda, moreover the possibility to cause fear in the public is very narrow as discussed above, terrorist groups still tend to carry out their attacks outside of cyberspace (Haig & Kovács, 2007).

Terrorist activity in cyberspace seems to remain subsidiary to armed attacks and their primary aim is to assist the functioning of the terrorist group via cybercrimes. As an exception, spreading terroristic propaganda and broadcasting dangerous information (former aimed the general public with the goal to recruit new members, the latter at the members of a terrorist group, e.g. how to make a bomb) are unique to terrorist groups and both are committed on the Internet on a large scale. As an example, the cyber forces of al-Qaeda, named the digital jihad, are very active on the not overly ruled and blue-penciled sites of social media, such as on Twitter (Kovács & Illési, 2011).

Secondly, cyberterrorism and cyber warfare need to be differentiated as well. According to Dornfeld, the main dissimilarity can be found in the fact, that cyber warfare is always connected at least to one state, whereas cyberterrorism has no element of state authority. But then again, even though this distinction exists on a theoretical level, in practice no state is willing to admit to a cyberattack carried out in peace time. Valerie and Knights also point out the close connection of cyberattacks against national critical infrastructures carried out by terrorist groups and opposing nations (Valerie & Knights, 2000). Naturally, the scale and intensity of a cyberattack by a state will presumably always be much higher, than as of a terrorist group, however the author would like to point out, that cyber warfare is closely connected to cyberattacks only. In other words, cybercrimes via the Internet, also known as soft cyberterrorism (Kovács & Illési, 2011), such as money laundering or drug trafficking, which make up most of the current cyber activities of terrorist groups, will not be carried out by a state authority.

Cyberterrorism and International law

In the last few decades, numerous international and regional treaties came to life in connection with the fight against terrorism. According to Kecskés, these agreements can be divided into two groups (Kecskés, 2019). On one hand, there are those agreements that are universal in nature, meaning they were not created specifically for terrorist activities, however, they regulate actions typically committed by terrorist groups. These are the following:

- 1963 Convention on Offences and Certain Other Acts Committed on Board Aircraft.
- 1970 Convention for the Suppression of Unlawful Seizure of Aircraft.
- 1971 Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation.
- 1988 Protocol for the Suppression of

Unlawful Acts of Violence art Airports Serving International Civil Aviation.

- 1973 Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons.
- 1979 International Convention against the Taking of Hostages.
- 1979 Convention on Physical Protection of Nuclear Material.
- 1988 Convention for the Suppression of Unlawful Acts Against the Safety of Martitime Navigation.
- 1988 Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf.
- 1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection.
- 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation.
- 2010 Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft.
- 2013 Arms Trade Treaty.

On the other hand, there are three conventions, specifically regulating terrorism, namely:

- 1997 International Convention for the Suppression of Terrorist Bombings
- 1999 International Convention for the Suppression of the Financing of Terrorism
- 2005 International Convention for the Suppression of Acts of Nuclear Terrorism

According to O'Donnell, who discusses the complicated system of international treaties on terrorism in great detail, the main and common goal of the treaties is to obligate the ratifying states to implement the crimes defined by the treaties into their respective domestic criminal laws and to punish these crimes with an appropriate sentence in light of the gravity of the crime committed (see: O'Donnell, 2006). Further aim of the treaties is to define jurisdiction for the crimes in the treaty in question. Jurisdiction in these multilateral agreements is based on territoriality, on the nationality of the offender and the victim, and in some cases on the presence of the attacker in the territory of the state (O'Donnell, 2006).

The treaties define a large number of offences, such as crimes against civil aviation, crimes against the person, and crimes committed in connection with a bomb or nuclear material (O'Donnell, 2006). There are two crimes in connection with the financing of terrorism as well. Unfortunately, however, with the exception of the Protocol Supplemental to the Convention for the Suppression of Unlawful Seizure of Aircraft and the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation, none of the multilateral treaties from above expressively mention cyberattacks (Fidler, 2016).

Shiryaev analyzed the different sources of terrorist threats in light of the main question, whether certain terrorist attacks impose a real threat in the realities of cyberspace (Shiryaev,

2013). For reasons of space, only those aspects will be covered here, that are the subject of the three main conventions on terrorism.

Terrorist bombings

According to Article 2 (1) of the International Convention for the Suppression of Terrorist Bombings *"any person commits an offense within the meaning of this Con-vention if that person unlawfully and intentionally delivers, places, discharges or detonates an explosive or other lethal device in, into or against a place of public use, a State or government facility, a public transportation system or an infrastructure facility: a. With the intent to cause death or serious bodily injury; or b. With the intent to cause extensive destruction of such a place, facility or system, where such destruction results in or is likely to result in major economic loss"*. Shiryaev argues that one cannot commit such a crime through delivering or placing, since the physical interaction with the bomb is cyberspace is impossible, however, he acknowledges the realities of discharging or detonating a bomb through cyber means, in which case a cyberattack could have the capability to cause death, serious bodily injury or substantial material damage (Article 1(3) of the International Convention for the Suppression of Terrorist Bombings). As an example of such an attack, Shiryaev references Cohen and points to the possibility of an attack against computers at nuclear reactors and biological labs, which would evidently lead to a disaster sufficing the legal requirements from above.

Financing terrorism

The International Convention for the Suppression of the Financing of Terrorism from 1999 prohibits the provision or collection of funds in order to carry out terrorist acts. Shiryaev expresses the view, that the scope of this Convention is very limited in connection to cyberterrorism, since according to him, it would only be applicable in the unlikely event, that someone's bank account is broken into through a cyber-attack with the intent of transferring money to terrorists, or acquiring it for further use. In the authors opinion, however, cyberterrorism is not limited to cyber-attacks, but it includes soft cyber-terrorist acts described above as well. As a consequence, the Convention on Financing Terrorism would apply to cyberterrorism in cases of cybercrimes carried out via Internet for the purpose of collecting funds.

Acts of Nuclear terrorism

Shiryaev points out that based on the terms used in the Convention on the Physical Protection of Nuclear Material (e.g. possession, use, transfer, theft, fraudulent obtaining, moving; Article 7 (1) (a)-(c) Convention on the Physical Protection of Nuclear Material) of nuclear material, the possibilities of cyberterrorism in connection to nuclear material are very limited. Nevertheless, it is not totally impossible, since similarly to the cyber-attack of the IT infrastructures of a biological lab, the target of such an attack can be a nuclear reactor as well, which if carried out successfully, has a very high chance of causing death, serious injury, or substantial damage to property.

Just like the Convention on Nuclear Material, the International Convention for the Suppression of Acts of Nuclear Terrorism also contains multiple physical acts (e.g.

possessing radioactive material) that stay irrelevant in the context of cyberterrorism, but it also prohibits the damaging of a nuclear facility, which then leads to the (possibility of) dispersal of radioactive material. It must be noted that the cyberattack is to be qualified as a terrorist attack based on the intent alone, to compel a natural or legal person, an international organization, or a state to do or refrain from doing any act.

Shiryaev argues, that the case of Stuxnet, where the suspects Israel and the USA attacked the nuclear facilities of the Islamic Republic of Iran by means of a cyber-attack, is the first ever act of nuclear cyberterrorism, since the act hold the risk of dispersal of radioactive material, therefore it must have been seen as a breach of the rules of the Convention on Nuclear Terrorism, however neither Israel, nor the USA were part of the Convention on Nuclear Terrorism.

Cyberterrorism in regional agreements

Besides these international treaties, there are various regional agreements as well, that are essential for counter-terrorism in the European region (Kecskés, 2019). These are the following:

- 1977 European Convention on the Suppression of Terrorism.
- 2001 Convention on Cybercrime.
- 2003 Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems.
- Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration.
- 2005 Council of Europe Convention on the Prevention of Terrorism.
- 2005 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism

In terms of regulating cyberterrorism, from the list above the Council of Europe's Convention on Cybercrime from 2001, also known as the Budapest Convention, is the most relevant source of law. 48 countries have joined the Budapest Convention, mostly European countries with a few exceptions, such as Russia, Turkey, and Switzerland. The Budapest Convention aims at the harmonization of domestic criminal law on cybercrime committed via Internet or with other computer networks. Unfortunately, the Budapest Convention fails to regulate cyberterrorism, therefore it can only be seen as useful for cases of soft cyberterrorism, not however for so called hard cyberterrorism.

A long-awaited, new era of regulating terrorism could come once the Comprehensive Convention on International Terrorism is agreed upon (De Vido, 2017). The United Nation's Ad Hoc Committee was established

as back as 1996, but the last meeting of the Committee to work on the draft of the convention took place in 2013. Unfortunately, the negotiations are currently still deadlocked, the reason being, no consensus could be found regarding the definition of terrorism.

The current system of treaties on conventional terrorism is quite confusing and perplexing, which leads to a general uncertainty. The general approach of international law concerning the matter is to regulate as much as possible on a national level, which considering the international nature of cyberspace, is very counterproductive.

In the authors view, the following problems can be identified in connection with the international regulation of cyberterrorism:

- The identification of the attacker(s) can be very challenging, which can be the determination of jurisdiction as well as the enforcement of the law especially difficult.
- The cases are very limited, where a cyberterrorist attack reaches the level of offences of conventional terrorism. Death, serious body injury, serious damage to property, or property damage that causes major economic loss are not impossible, but rather hard to achieve by cyber means.
- The insufficient regulatory framework on cyberterrorism could and possibly will lead to the application of cybercrime norms on cyberterrorist cases, if somewhat plausible. As Fidler points out, this is against the general state interest, according to which terrorism in general needs to be distinguished from other crimes, not just in 'reality', but in cyberspace as well.

In summary, in light of the above, the author agrees with Fidler, who stated that international law on terrorism in its current form is not well applicable to cyberterrorism (Fidler, 2016). For certain cases, some of the treaties can be applied using a broad interpretation, however, a lot if cyberterrorist activity is left out, and stays unregulated.

Cyberterrorism and International Humanitarian Law

The connection between cyberterrorism and international humanitarian law is out of the scope of this paper, however, it is important to mention that following the events in Estonia in 2007 and the cyber-conflict between Russia and Georgia, as a response the North Atlantic Treaty Organization (NATO) established the NATO Cooperative Cyber Defence Centre of Excellence in Estonia, and the Tallinn Manual on the International Law Applicable to Cyber Warfare was released in 2013. It was followed by the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations in 2017 (Additionally, the Tallinn Manual 3.0 is currently being worked on.). Both of the Manuals lay down the basic principles for the application of law of war in cyberspace, and analyze the possibilities, how the current framework of international law could be applied on cyberattacks, or on a potential cyberwar. None of the Manuals have binding effect, and they have been criticized for being too vague, nevertheless, they are the first legal cornerstones for a potential future cyber war.

The fight against cyberterrorism in the EU

The European Union Terrorism Situation and Trend Report from 2020 (TE-SAT) (Europol, European Union Terrorism Situation and Trend Report (TE-SAT) 2020, 2020) is the Europol's annual overview on the terrorist activities. In its latest version from 2020, in addition to the Global Terrorism Index 2020 (IEP, 2020), the following recent data can be obtained on terrorism:

In 2019 there were a total of 119 completed, failed and foiled terrorist attacks and 1004 arrests across Europe, the United Kingdom having the most terrorist cases (64 attacks, 281 arrests). Interestingly, Spain had the second highest number of arrests (224), but only 7 attacks, whereas Germany was attacked just three times and 35 individuals were arrested. Most cases can be linked to ethno-nationalist and separatists (57), left-wing groups (26), and jihadists (21), however, all ten people who died and 26 out of 27 who were injured, were victims of jihadist attacks.

In accordance with this data, the United Kingdom is the first among the European countries with the rank 30 on the chart of the latest Global Terrorism Index, which yearly measures the impact of terrorism in 135 countries. Next is France (rank 38), then Greece (rank 44), and the third is Germany (rank 48). In terms of the level of impact of terrorism the United Kingdom, France and Greece are on level medium, and Germany is only on level low.

From the Internet Organised Crime Threat Assessment 2020 (IOCTA 2020) (Europol, 2020), also provided by the Europol on a yearly basis, additional data can be obtained regarding cybercrime activities in the year 2019. According to the IOCTA 2020, ransomware remained the most dominant threat both in the public as well as in the private sector. The second biggest threat proved to be malware attacks in the broader sense, such as banking Trojans and at third place were DDoS attacks, which are known as a major security threats in the critical infrastructure sector (Mezei, 2018).

As Kasznár pointed out, there are new tendencies to be seen regarding the terrorist activities in Europe (Kasznár, 2018). Kasznár mentions the significant changes in the acts and general functioning of terrorist groups in recent years, also the rising tendencies of new organizations parallel to the constantly growing activity of the old, major terrorist groups. Heffelfinger also points to the cybersecurity risks connected to the modern day jihad (Marsili, 2019).

In the authors opinion, in terms of cybersecurity risks connected to terrorist threats, there are two points to be made here. First of all, as mentioned above, terrorist groups do not show a great interest in attacking the cyber infrastructure of critical infrastructures yet. However, major international terrorist groups do have the financial means to take part in armed conflicts, to work together with transnational criminal organizations (Ivanov, 2014) and therefore unquestionably to hire professional hackers, qualified enough for such a high-level attack, moreover they are motivated more than ever to recruit new members from Europe (Répási, Az Európai Unión belüli terrorizmus tendenciái és jellegzetességei a TE SAT 2018 kiadvány tükrében, 2018). Additionally, since

the 2000s, there is a growing tendency of lone wolf terrorism in North-, Western-, and South-Europe (Répási, 2014) therefore prevention and detection play an important role in an effective national cybersecurity system (Papp, 2018). It can be presumed that it is only a question of time, when the attacks will come, not whether they come at all.

Another possibility for major terrorist groups is to qualify their own members, which solves the issue with purely financially motivated hackers not wanting to work for a terrorist group, even though it is unquestionably time-consuming since it takes multiple years of training.

The second consideration to be made is that with the recently rising number of new terrorist organizations, there is a high chance of the rise of cyberterrorist groups, that are purely active in cyberspace. This could bring a whole new era of counterterrorism challenges both in Europe and in the rest of thew world. Newly established, smaller organizations will hardly have the same human and financial recourses as big terrorist groups though, therefore their activities will presumably be limited to Internet based cybercrimes and cyberattacks against uncomplicated, not highly secured information systems, at least in the beginning years.

The basis for the regulatory framework on terrorism in the EU gives Title VII. Article 222 as well as Title V Chapter 1 Article 67 and 75 and Chapter 4 Article 83 of the Treaty on the Functioning of the European Union (TEFU) (Pék, 2020). According to the solidarity clause of Article 222.:

The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States, to:

(a) - prevent the terrorist threat in the territory of the Member States; - protect democratic institutions and the civilian population from any terrorist attack; - assist a Member State in its territory, at the request of its political authorities, in the event of a terrorist attack;

(b) assist a Member State in its territory, at the request of its political authorities, in the event of a natural or man-made disaster.

As Pék pointed out, neither the TEFU, nor other regulations that were based on these articles use common terms regarding terrorism, moreover, the various definitions (such as terrorist attack, terrorist threat) used by them are not defined either. Unfortunately, the regulatory practice of the EU follows the international trend, which consequently leads to a much lower level of efficiency.

The Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism was the first legal act by the EU that regulated the fight against terrorism in the Union. 15 years later in 2017 came the Directive 2017/541 of the European Parliament and of the Council on combating terrorism, which then replaced the said Council Framework Decision. The Terrorism Directive defines the terms funds, legal person and terrorist groups in its Article 2. According to Title II. Article 3. Paragraph 1. and 2. of the Terrorism Directive Member States must take the necessary measures to ensure that various intentional acts, as defined as offences under national law, which, given their nature or

context, may seriously damage a country or an international organization, are defined as terrorist offences in case they are committed with the aim to

- seriously intimidate a population;
- unduly compel a government or an international organization to perform or abstain from performing any act;
- seriously destabilize or destroy the fundamental political, constitutional, economic or social structures of a country or an international organization.

The list of terrorist offences is exhaustive and includes amongst others the fol-lowing cases that have the most relevance to cyberterrorist activities in the authors opinion:

- extensive destruction of an information system likely to endanger human life or result in major economic loss
- seizure of aircraft, ships or other means of public or goods transport
- release of dangerous substances, or causing fires, floods or explosions, the effect of which is to endanger human life
- illegal system interference, and illegal data interference
- the threat to commit any of these acts.

The Directive includes cases when the attack is purely directed against an infor-mation system with the intent of disruption or destruction, however, in light of the considerations made above regarding the multilateral treaties on international terrorism, other cases of terrorism can be committed by means of a cyber-attack as well. Evidently, the possibility of the seizure of an aircraft through a cyber-attack is currently enormously low, however, it is important that the regulatory framework is flexible enough, that in case such events occur, the attack can be qualified and reacted to accordingly as an act of terror.

The second important source of law is the Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems, which by replacing the Council Framework Decision 2005/222/JHA on attacks against information systems advanced and strengthened the regulatory framework (Oleksiewicz, 2017). The main aim of the Directive was to establish a common approach to criminal offences in respect of attacks against information systems. According to Preambulum 10 of Directive 2013/40/EU the *„penalties should be effective, proportionate and dis-suasive and should include imprisonment and/or fine."*

The Directive provides for criminal penalties only for cases that are not minor, but the Member States have the competence to determine what constitutes a minor case according to their national law and practice. The Directive regulates the following cases of cybercrime:

- illegal access to information systems
- illegal information system interference
- illegal data interference
- illegal interception of computer data to, from or within an information system, including electromagnetic emissions

According to Article 9 of the Directive 2013/40/EU all the offences from the list above must be punishable by a maximum term of imprisonment of at least two years, whereas in cases of aggravating factors, the punishment must be at least five years of

imprisonment. Such an aggravating factor is, when the perpetrator(s) commit illegal system interference, or illegal data interference against a critical infrastructure information system.

In summary, the current European tendencies regarding regulating terrorism do not differ from the broad framework of international law. For now, the clear focus on cybercrime does not seem to cause legal issues, since terrorist activities are still restricted to broadcasting propaganda and fundraising via Internet-based cybercrimes, however, once cybercrime becomes an active national security risk factor, the regulatory deficiencies will be clear and they will cause legal and law enforcement issues as well. In the author's opinion, it would be absolutely necessary to for the EU to regulate cyberterrorism on a deeper level. Instead of only focusing on cybercrime, potentially committed both by cybercriminals as well as by cyberterrorists, the EU needs to recognize the fact that it is only a matter of time until the lack of a clear, detailed regulatory framework on cyberterror leads to a disastrous outcome. Potential areas of regulatory and security policy development could be the following:

- creating the Convention on Cyberterrorism modeled on the Convention on Cybercrime, within the framework of which regulations regarding national cyberterrorism jurisdiction, as well as the different types of cyberterrorist activities and their minimum sentence could be established;
- addressing terrorist activity on social media through restrictive regulatory measures, especially the propaganda directed at the younger generations of Muslim faith living in Europe with the goal of lowering the risk of their recruitment;
- establishing an adequate, higher level of security for newer technologies (such as cloud services, and Internet of Things services) in cases, where they are used by actors of the public sector;
- since terrorists mainly attack innocent people, this tendency will presumably not change in cyberspace either, therefore it would be also fundamental to raise general awareness of potential cyber-threats linked to terrorist organizations on a European, as well as on a national level.

Cyberterrorism in Hungary

According to Simon, considering the organizational structure of the units fighting cybercrime, with the goal of an optimal allocation of data, the following categories can be created in Hungary (Simon, 2018):

- cyber attacks
- bankcard frauds
- online sexual exploitation of children
- cybercrimes against intellectual property
- other types of frauds committed online.

However, Simon acknowledges the fact described by the author above, that no hard lines can be drawn between the various types of cybercrime, hence their interlacing character (Simon, 2018). Therefore, in case of cyberterrorist activity, no one specific law enforcement unit will be involved, but rather a handful, each investigating according to their specialty. As a consequence, besides questions in relation to dogmatics, in the

author's opinion differentiating between the different types of cybercrimes does only play a significant role once legal actions are pursued against an attacker, not however in the stages of defense, deflection, countermeasures, or cyber-investigations.

In Hungary, the main regulatory framework of cybercrime and cyberterrorism consists of multiple sections of the Act C of 2012 on the Criminal Code (hereafter referred to as: Criminal Code), as well as the Act L on Information Security of State and Local Government Bodies (hereafter referred to as: Information Security Act) and the Degree 233/2013 (VI. 30.). Additionally, the Act CLXVI. of 2012 on Critical Infrastructures and the Degree 65/2013. (III. 8.) need to be mentioned as the primary legislation on critical (information) infrastructure protection. In the following the author discusses the two main Sections of the Criminal Code, that have the most relevance considering the topic of this paper:

Section 314 of the Criminal Code: Acts of terrorism

For a long time, there was no specific Paragraph in Section 314 of the Criminal Code for terrorist acts committed in the cyberspace. This changed with the Act XLIII of 2020 which entered into force on 1 January 2021, which by adding litera i) to Section 314 Paragraph 4 widened the scope of the regulation. Since the beginning of this year terrorist acts can be committed with the breach of an information system or data as per Section 423 of the Criminal Code, in case the criminal offence endangers the public or involves the use of arms in order to

- coerce a government agency, another State or an international body into doing, not doing or countenancing something,
- intimidate the general public,
- conspire to change or disrupt the constitutional, economic or social order of another State, or to disrupt the operation of an international organization (Section 314 Par 1 of the Criminal Code).

In light of the above, for cyberterrorism the endangerment of the public is of relevance rather than the use of arms.

Section 423 of the Criminal Code: Breach of information system or data

Pursuant to Section 423 Paragraph 1 of the Criminal Code any person, who gains unauthorized entry to an information system, disrupts the use of the information system unlawfully or by way of breaching his user privileges, or alters, deletes, or renders inaccessible without permission or by way of breaching his user privileges data in the information system can be sentenced up to two years. Paragraph 3 specifies the aggravating circumstance, when the criminal offense is committed against works of public concern. In light of Section 459 Point 21 of the Criminal Code, which defines works of public concern, unfortunately the term used by the Criminal Code is not equivalent to the definition of critical infrastructures, therefore in cases when for example the healthcare facilities are targeted (Mezei, 2018).

Other important cybercrimes that could be of relevance in the context of cyberterrorism are the following:

- Section 375 of the Criminal Code: Information system fraud
- Section 422 of the Criminal Code: Illicit access to data
- Section 424 of the Criminal Code: Compromising or Defrauding the Integrity of the Computer Protection System or Device

As mentioned above, the laws regulating the defence of information systems of critical infrastructures, that are possible targets of cyberterrorists, are on one side the Information Security Act and the Degree 233/2013 (VI. 30.) in connection to it, as well as the Act CLXVI of 2012 on Critical Infrastructures and the Degree 65/2013 (III. 8.). According to the Information Security Act, all critical infrastructures regulated in the Act CLXVI of 2012 are also subject of this Act. Unfortunately, the Information Security Act does not regulate any cyber-defence measures for the information system of critical infrastructures, it only promotes the coordination and cooperation between the different cybersecurity organizations (Simon, 2018).

Conclusions

Cyberterrorism is still a very new aspect of international and national security threat landscape and it takes time until the regulatory frameworks will be adapted to the new challenges. In the current state of international law on terrorism, the international co-operation in case of a cyberterrorist attack would be difficult and time-consuming. In light of the current regulatory framework, each state has to secure its own cyberspace, regardless the fact that cyberspace and the risks and threats connected to it are of international nature, therefore, an effective defense system is unimaginable without cooperation and clear jurisdictions. The long-awaited Comprehensive Convention on International Terrorism could be a major step towards a secure cyberspace, however as indicated above, it may take years, until an agreement is made on questions like the definition of terrorism. The author presents multiple key areas of potential development that could lead to a much safer cyberspace in the European region. The most fundamental would be a Convention on Cyberterrorism, which could be a modern version of the Budapest Convention of 2001, however, focusing on cyberterrorism. Establishing clear guidelines on jurisdiction, and sentencing could be major (cyber-)security policy steps for Europe. But the author argues also, that since terrorist attacks target the innocent, and through the Internet and general digitalization of the world, it is easier than ever to attack the general public on a large scale, it is fundamental that besides the military-focused international measures of the NATO, the EU focuses on the civil aspects of cyberterror (e.g. social media; raising awareness to the importance of cybersecurity from the aspects of terror) as well.

Regarding the laws of Hungary on cyber-terrorism, it needs to be pointed out, that even though the regulatory framework is not flawless, and more work is needed, especially in the sector of critical information infra-structure protection, it is in accordance with the current European standards. Further-

more, the widening of the scope of Section 314 of the Criminal Code can be regarded as forward-looking, and promising. With the help of this change, law enforcement is able to categorize and react to a potential cyber-terrorist attacks as such, as a consequence of which, a more secure national cyberspace is established.

References

Cohen-Almagor, R. (2018). Cyberterrorism. In B. Warf (ed.), *SAGE Encyclopedia of the Internet* (old.: 169-171). Thousand Oaks: SAGE Publications Inc. http://dx.doi.org/10.4135/9781473960367

De Vido, S. (2017). The future of the draft UN Convention of international terrorism. *Journal of Criminological Research Policy and Practice*, 233-247. DOI: 10.1108/JCRPP-09-2016-0020

Dornfeld, L. (2019). Kiberterrorizmus – a jövő terrorizmusa? In K. Mezei, *A bűnügyi tudományok és az informatika* (old.: 46-63). Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont. Link: https://jog.tk.hu/uploads/files/03_buntetojog_informatika_DORNFELDL.pdf.

Europol. (2020). Forrás: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Europol. (2020). *European Union Terrorism Situation and Trend Report (TE-SAT) 2020*. Forrás: https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020

Fidler, D. (2016). Cyberspace, Terrorism and International Law. *Journal of Conflict & Security Law*, 2. https://doi.org/10.1093/jcsl/krw013

Haig, Z., & Kovács, L. (2007). New way of terrorism: Internet- and cyber-terrorism. *AARMS*, 659-671. Link: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.454.9045&rep=rep1&type=pdf

IEP. (2020). *Global Terrorism Index 2020*. Forrás: https://visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-1.pdf

Ivanov, E. (2014). Combating Cyberterrorism under International Law. *Baltic Yearbook of International Law*, 55-69. https://doi.org/10.1163/22115897-90000120

Kasznár, A. (2018). New Tendencies in the Terrorist Attacks Against Europe. *Hadtudományi Szemle*, 142-153.

Kecskés, G. (2019). A nemzetközi jog eszközrendszere a terrorizmus elleni küzdelemben. In R. Bartkó (ed.), *A terrorizmus elleni küzdelem aktuális kérdései a XXI. században* (old.: 81-97). Budapest: Gondolat Kiadó.

Kovács, L., & Illési, Z. (2011). Cyberhadviselés. *Hadtudomány*, 4. Link: http://mhtt.eu/hadtudomany/2011/1/HT-2011_1-2_5.pdf

Marsili, M. (2019). The War on Cyberterrorism. *Democracy and Security*, 172-199.

https://doi.org/10.1080/17419166.2018.1496826

Martinez, E. (2016). *Globalization and the 'Fourth Wave': Contemporary International Terrorism in a Comparative-Historical Perspective*. Link: https://stars.library.ucf.edu/cgi/viewcontent.cgi?article=1045&context=honorstheses

Mezei, K. (2018). A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. *Pro Futuro*, 66-83. https://doi.org/10.26521/Profuturo/2018/1/4674

Mikac, R., Mamic, K., & Zutic, I. (2020). *Cyberterrorism Threats to Critical Infrastructure: Coordination and Cooperation from Brussels to South- Eastern Europe and back*. Forrás: https://www.bib.irb.hr/1088286

O'Donnell, D. (2006). International treaties against terrorism and the use of terrorism during armed conflict and by armed forces. *International Review of the Red Cross*, 853-880. https://doi.org/10.1017/S1816383107000847

Oleksiewicz, I. (2017). A legal assessement of management of the European Union cyberterrorism policy. *Modern Management Review*, 141-152. DOI: https://www.doi.org/10.7862/rz.2017.mmr.32

Papp, Z. (2018). *A kiberterrorizmus módszerei, lehetséges eszközei és az ezek ellen történő védekezés alternatívái*. Budapest. Link: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/Papp_Zoltan_PhD_ertekezes_terveze te.pdf

Pataki, M., & Kelemen, R. (2014). Kiberterrorizmus. A terrorizmus új arca. *Magyar Rendészet*, 103-116. https://folyoirat.ludovika.hu/index.php/magyrend/article/view/3886/3145

Pék, R. (2020). Terrorizmus és terrorizmus elleni küzdelem az Európai Unióban és a terrorizmus fogalmának értelmezési problémái. *Doktoranduszok Országos Szövetsége*, (old.: 147-155). Budapest. https://doi.org/10.38146/bsz.2020.6.3

Répási, K. (2014). *A terrorizmus az Európai Unióban*, 20-40. Link: http://www.nemzetesbiztonsag.hu/cikkek/nb_2014_3_05_repasi_krisztian.pdf

Répási, K. (2018). Az Európai Unión belüli terrorizmus tendenciái és jellegzetességei a TE SAT 2018 kiadvány tükrében. *Nemzeti Közszolgálati Egyetem - Stratégiai Védelmi Kutatóközpont Elemzések*, 1-15. Link: http://www.nemzetesbiztonsag.hu/cikkek/nb_2018_3_08_repasi.pdf

Shiryaev, J. (2013). Cyberterrorism in the Context of Contemporary International Law. (old.: 139-191). Research Paper No. 2012/03: Warwick School of Law. Link: https://digital.sandiego.edu/ilj/vol14/iss1/5

Simon, B. (2018). A rendészeti szervek együttműködése a kiberbűnözés ellen. *Nemzetbiztonsági Szemle*, 36-58. Link: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1510/828

Tóth, Z. (2016). Az Iszlám Állam online térhódítása. *Nemzetbiztonsági Szemle*, 26-42. Link:

https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1881/1169

Valerie, L., & Knights, M. (2000). Affecting Trust: Terrorism, Internet and Offensive Information Warfare. *Terrorism and Political Violence*, 15-36. Web: https://doi.org/10.1080/09546550008427547