SECURITY DIMENSIONS
INTERNATIONAL & NATIONAL STUDIES
NO. 25; 2018 (118–130)
DOI 10.24356/SD/25/6

FROM TERRORISM TO CYBERTERRORISM

PROF. ING. VLADIMÍR SMEJKAL, CSC., LL.M.
Moravian University College Olomouc, CZECH REPUBLIC

ABSTRACT

The paper deals with a new phenomenon of crime – the terrorism in cyberspace. Terrorism, cyberterrorism and cyberwar are defined here. The paper focuses on the systemic integration of cyberterrorism into the structure of terrorist attacks, describes various types of attacks in cyberspace, and deals with the legal definition of cyberterrorism.
Since the 1990´s, war and armed conflict have been moving increasingly from the interstate to the intrastate area. In the postmodern conflict, besides government troops, various irregular paramilitary groups, most commonly defined tribally, ethnically, or religiously, keep on fighting. However, their military activities are usually linked to a large-scale criminal activity.

Whereas, in standard wars, we expect states and their armed forces to be parties to the conflict, in the case of the postmodern conflict, hybrid wars, and the so-called asymmetric threats, war is not separated from the life of the civil society, as it used to be in standard wars of the 20th century. It is also increasingly difficult to separate war and terrorist attacks.

Cyberattacks are becoming a part of terrorist attacks. Modern information technologies are becoming more and more important in spreading ideologies which provide a fertile ground for terrorism, as they are increasingly important for training and teaching terrorist practices. Terrorists use the Internet as a means of spreading propaganda aimed at recruiting sympathizers as well as instructions and manuals for training or attack planning. Cryptocurrencies such as bitcoins are used to transfer finances.

In this context, cyberterrorism could be defined as the use of the means of modern information and communication technologies to implement an act of violence, in order to provoke a certain reaction (from the point of view of terrorists, in ideal case, the by them required psychological reaction) of the audience of the terrorist act. In the case of cyberterrorism, it would be a politically motivated attack on instruments and / or the process of obtaining and / or processing electronic data which, as a result, means violence against non-military targets and the purpose of which is to influence, in a certain way, a wider circle of recipients rather than the direct victims of such an attack.

While mostly natural persons are the target of typical terrorism, in the case of cyberterrorism, on the contrary, the attacks are aimed at state authorities, corporations, and the critical infrastructure. It is a question whether in these cases we are able to correctly assess whether it is a terrorist attack or an (unreported) information or cyberwar conducted by a foreign state. In some cases, we cannot even be sure whether it is a criminal act which is masked as a terrorist one or vice versa, which is easier to do in cyberspace rather than in the material world.

ARTICLE INFO

Article history
Received: 10.01.2018 Accepted 29.01.2018

Key words
terrorism, cyberterrorism, information war, cyberwar, Czech Cyber Security Act, cybercrime

Introduction

Today, whenever any act of violence (against people and / or against property) occurs anywhere in the world, one of the first questions that is dealt with is whether it was an ordinary crime or an act of terrorist. This corresponds to standard criminal procedures in which we try to define the following aspects in formulating the criminological characteristics of the crime: 1. the way in which the crime was perpetrated, 2. the criminal situation, 3. the personality traits of the perpetrator, 4. the characteristics (personality traits in the case of people) of the target of the attack (the victims) of the crime, 5. the motive for the crime. This is the only way in which the perpetrators can be traced, evidence can be obtained and the matter can be brought before the court. The issue of prevention, which must take account of all the criminalistic characteristics mentioned above in order to be a successful measure, is also essential. Similar procedures must be applied if the fight against terrorism (and therefore cyberterrorism) is to be successful.

From classic crime to cyberterrorism

There are many definitions of terrorism. One of the better-known definitions is, for example, the definition formulated as early as the 1980s in the US according to which "Terrorism is the use of violence or the threat of violence especially against civilians in the pursuit of political aims, religious, or ideological change. Terrorism also includes criminal offences that

are symbolic in nature and are a means of achieving objectives other than those on which the crime is focused"[1].

The definition of A. P. Schmidt interprets terrorism as follows: "Terrorism is an anxiety-inspiring method of repeated violent action, employed by (semi-)clandestine individual, group, or state actors, for idiosyncratic, criminal, or political reasons, whereby –in contrast to assassination – the direct targets of violence are not the main targets. The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative or symbolic targets) from a target population, and serve as message generators. Threat- and violence-based communication processes between terrorist (organization), (imperilled) victims, and main targets are used to manipulate the main target (audience(s), turning it into a target of terror, a target of demands, or a target of attention, depending on whether intimidation, coercion, or propaganda is primarily sought"[2].

The European definition can be found in Article 1 of the Framework Decision of the Council of the European Union of 13 June 2002 on Combating Terrorism[3]. According to the European definition,

> terrorist offences are considered deliberate acts which given their nature or context, may seriously damage a country or an international organisation where committed with the aim of: seriously intimidating a population; or unduly compelling a government or international organisation to perform or abstain from performing any act; or seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation:
> (a) assaults that threaten human life with the possible consequence of death,
> (b) attacks that threaten the personal integrity of a human being,
> (c) kidnapping or taking of hostages,
> (d) causing extensive damage to government or public facilities, the transport system, and the infrastructure, including the information system,

[1] M. Brzybohatý, *Terorismus I.*, Vydavatelství Police History, Praha 1999; Ministry of the Interior of the Czech Republic, http://www.mvcr.cz/clanek/definice-pojmu-terorismus.aspx.

[2] A. P. Schmid, *Problémy s definováním terorismu,* [in:] *Encyklopedie světový terorismus. Od starověku až po útok na USA,* Svojtka & Co, Praha 2001.

[3] *Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA)*, „Official Journal L", 22/06/2002, no. 164, p. 0003–0007.

a fixed platform on a continental shelf, a place of public use or private property that may endanger human life or result in significant economic losses,
(e) seizure of an aircraft, ship or other means of public or freight transport,
(f) manufacture, possession, acquisition, transport, delivery or use of weapons, explosives or nuclear, biological or chemical weapons, as well as the research and development of biological and chemical weapons,
(g) the discharge of dangerous substances, arson, causing of floods or the detonation of explosives with the effect of endangering human lives,
h) suspension or interruption of the supply of water, electricity or another basic natural resource with the effect of endangering human lives,
(i) threats of perpetrating any of the acts referred to in points (a) to (h).

An important part of terrorist tactics is to achieve the greatest possible publicity with the purpose of generating fear.

The manifestations of terrorism include many forms of deliberate acts, including, but not limited to, extensive damage to government or public facilities, the transport system, and infrastructure, including the information system, or the disruption or suspension of the supply of water, electricity or other basic natural resources with the effect of endangering human lives[4].

We have previously defined cybercrime as a crime in which the computer, or only some of its components, plays a certain role as a body of technical and software equipment (including data), namely as:

1. **the object of such a criminal act**, with the exception of criminal acts whose object is movable property,
2. an **instrument of a criminal act**[5].

Today, attacks occur in cyberspace comprised of computer networks and the individual elements of these networks that have an IP address assigned to them. Therefore, this does not include only computers, but anything that can communicate with other elements in cyberspace through a TCP / IP or other protocol (e.g. security cameras or home appliances have been used). It can, therefore, be concluded that **cybercrime is a criminal act that takes place in cyberspace.**

According to § 2 point a) of the Czech Cyber Security Act No. 181/2014 Coll., *cybernetic space is a digital environment enabling the creation, process-*

[4] *Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA)*, „Official Journal L", 22/06/2002, no. 164, p. 0003–0007, or § 311 of Act No. 40/2009 Coll., Penal Code, as amended.

[5] V. Smejkal, T. Sokol, M. Vlček, *Počítačové právo,* C. H. Beck, Praha 1995.

ing and exchange of information consisting of information systems and electronic communication services and networks. According to the explanatory report to the bill, the concept of cyberspace is defined as "an information environment for the realization of information transactions which consists of technologies whose definitions and conditions of use are regulated by special laws, i.e. information systems, services and electronic communication networks". They are also information systems, services and electronic communication networks that are not connected to a public network, i.e. to the Internet. Also the European Union works with the terms "cyberspace" (i.e. "cybernetic space") and "cybercrime". For example, the European Centre for Combating Cybercrime (EC3) was established at Europol at the beginning of 2013[6].

As with cybercrime, we will talk about terrorist attacks that take place in cyberspace in the case of cyberterrorism as well. In doing so, we can distinguish whether the target of the attack is only in cyberspace (an attack on a server), or whether an attack that takes place in cyberspace will have an impact on the physical world. In particular the acts under point d) above are related to cyberterrorism, but the use of information technology for the attacks under points a), b), e), g) and h) above cannot be ruled out either, depending on the extent to which the infrastructure is dependent on the information technologies. An example is the closure of the oxygen supply to patients in an intensive care unit or making changes in a particular transport system with the aim of causing disasters[7].

According to Denning, cyberterrorism is the convergence of cyberspace and terrorism. It consists in unlawful attacks and threats of attacks against computers, networks, and information stored in them with the aim of intimidating or forcing a government or its people to promote political or social goals. In order for an attack to be classified as an act of cyberterrorism, it should result in violence against persons or property or at least generate fear. Such attacks include, for example, attacks that lead to death or injury to health, explosions or severe economic losses, as well as attacks against the critical infrastructure[8].

[6] https://www.europol.europa.eu.

[7] V. Smejkal a kol., *Právo informačních a telekomunikačních systémů*, C. H. Beck, Praha 2004.

[8] Quoted by G. Weimann, *Cyberterrorism. How Real Is the Threat?*, „United States Institute of Peace, Special Report 119", December 2004. Available at http://www.usip.org/sites/default/files/sr119.pdf.

While the target of classical terrorism is mostly physical, the attacks are directed against state authorities, corporations, and the critical infrastructure in the case of cyberterrorism.

In these cases, there is the question of whether we can properly assess whether it is a terrorist attack or an (undeclared) information or cybernetic war conducted by a foreign state. In some cases, we cannot even be sure whether it is a criminal act masquerading as a terrorist act or vice versa, which is easier to achieve in cyberspace than it is in the material world.

In this context, **cybernetic terrorism (cyberterrorism) would therefore be the use of means of modern information and communication technology in order to implement an act of violence with the aim of inducing a certain psychological response in the audience of the terrorist act that is most desirable from the perspective of the terrorists.** To be more precise, cyberterrorism is a politically motivated attack on the instruments and/or the process of obtaining and/or processing electronic data (which in effect means violence against non-military targets) whose purpose is to have a certain influence on a circle of recipients wider than that of the direct victims of such an attack[9]. Cyber terrorism is a modern form of terrorism, the same as other forms of terrorist acts that are committed using specific means, such as chemical, biological, and nuclear terrorism.

The degree of publicity required for an act to be classified as cyberterrorism is a question to be asked. Perhaps this is the dividing line between cyberwar and cyberterrorism, because if we learn that the perpetrators are trying to completely conceal not only their identity but also the very fact that the act has occurred in a case being investigated, then it is either a criminal act or an information war[10]. However, the difference is not in the technological tools used, but in the context and the objective, i.e. in the motivation and profile of the perpetrators.

Beyond this contribution, also other forms of warfare that take place in cyberspace, which may be both a manifestation of terrorism and part of a declared or undeclared war, should be mentioned for a complete picture. Cybernetic warfare is intermingled with information warfare (IW),

[9] M. Bastl, *Kybernetický terorismus: studie nekonvenčních forem boje v kontextu soudobého válečnictví. Dissertation*, Masarykova univerzita v Brně, Brno 2007.

[10] W. L. Tafoya, *Cyber Terror,* „FBI Law Enforcement Bulletin", November 2011, available at http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror.

which includes in particular electronic warfare (EW) and information operations (IO). They are often used synonymously, but they are two subsets of multiple ways of conducting information warfare in the author's opinion. EW and IO include the use of cryptography and steganography, radar interference and electronic communication interference, altitude surveying, electronic tracking, the electronic acquisition of intelligence, etc.[11]

Cybernetic space has been classified as a new (5th) operational domain in international conflicts (in addition to land, water, air and space). In the so-called Tallin Manual, a cybernetic attack is defined as follows: "A cybernetic attack is an operation in cyberspace, whether it be offensive or defensive, which may reasonably be expected to cause personal injury or death or damage or destruction of things"[12].

Perpetrators

The immediate inducements of the behaviour of people and thus the perpetrators of criminal activities are motives, i.e. their hierarchical organization (motivation), consisting of internal inducements (needs) and external inducements (incentives). The motives supersede each other. Every human behaviour is thus motivated. There is no unmotivated behaviour; there is only behaviour with an unclear or unknown motivation. Not all motives are conscious. Unconscious needs may also be invoked in motivation.

In crime, two fundamental forms of criminal behaviour can be distinguished:

1. Programmed criminal behaviour, for which the victim's typing is typical, the preparation of tools, and the selection of the right situation are typical. As is the case with other human behaviour, an idea of the goal is formed, and in rare cases, the consequences are anticipated in the case of this behaviour. A plan is formulated and the aim is accepted. The actual criminal behaviour then takes place with the presence of feedback.
2. Reactive behaviour – behaviour that is not programmed whereby the situation is the decisive factor (a provoking person, presumably the victim), often aggressive sexual behaviour. There is no feedback in this

[11] V. Smejkal, *Kybernetická kriminalita*, Nakladatelství Aleš Čeněk, Plzeň 2015.

[12] *Tallinn manual on the international law applicable to cyber warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*, M. N. Schmitt (ed.), Cambridge University Press, Cambridge 2013.

case. The differences in the two forms of behaviour are not in the motives, but in the process of motivation[13].

Although reactive behaviour (an attack on a provocative hostage) may become a part of a terrorist act due to some external stimulus, most terrorist attacks will fall within the first area. In the case of cybernetic attacks, where the distance between the attacker and the target of the attack is even greater and is depersonalized, it can be supposed that this assumption is even closer to certainty.

The ten following characteristics relating to the opportunity to commit crimes are based on the general principle of "opportunity causes criminal activity":[14]

1. Opportunities are one of the causes of all crimes.
2. The opportunities to commit crimes are highly specific.
3. The opportunities to commit crimes are concentrated in certain locations and times.
4. The opportunities to commit crimes are based on the day-to-day movement of activities.
5. One type of crime [creates opportunities for others.
6. Some products offer more appealing opportunities to commit a crime.
7. Social and technical changes bring about new opportunities.
8. Crime can be prevented by limiting opportunities.
9. The limitation of opportunities does not usually lead to the relocation of the crime.
10. The targeted limitation of opportunities can lead to a more extensive reduction in the crime rate.

Two of the above-mentioned points (which could already be well-observed earlier, for example, in so-called white-collar crime) also apply to cybernetic crime, namely: *6. Some products offer more appealing opportunities to commit a crime* and *7. Social and technical changes bring about new opportunities*.

Computer crime (i.e. cybercrime) is still a very new area in the history of criminology. The acceleration of human society in the area of information technology is reflected in all fields: from trade and services, through art or eroticism, to public administration, and naturally in new forms of crime as well. Man is increasingly dependent on the (faultless) func-

[13] K. Netík, D. Netíková, S. Hájek, *Psychologie v právu*, C. H. Beck, Praha 1997.

[14] I. Matoušková, *Aplikovaná forenzní psychologie*, Grada Publishing, Praha 2013.

tion of information technologies, and the societal demand for the protection of these technologies from criminals is therefore growing. This demand is all the more important now that cybercrime has been associated with organized crime for over twenty years.

"Common criminals", who can work on their own so to speak, on order or in an organized crime group, have a motive (desire for profit), resources and people (whom they usually pay more than a bank or the state). They have the advantage of choosing the time and method, and the qualities and possibilities of information technologies play into their hands.

However, these criminals can operate as an organized group, or in some cases, as a part of an organized crime. *Organised crime is the recurrent (systematic) perpetration of target-oriented, coordinated serious criminal activity (and activities supporting this activity), whose involved entities are criminal groups or organisations (mostly with a multi-level vertical organisational structure) and whose main aim is to achieve the maximum illegal profits while minimising risk*[15].

The FBI defines organized crime as any group having some manner of a formalized structure and whose primary objective is to obtain money through illegal activities. Such groups maintain their position through the use of actual or threatened violence, corrupt public officials, graft, or extortion, and generally have a significant impact on the people in their locales, region, or the country as a whole[16].

Terrorism and organized crime have much in common. What differentiates them, however, is the financial motivation. While financial profit is the main goal in the case of organized crime, the financial issue is the basis for the further operation of terrorist groups and their preparation for warfare. Creating a strict definition of the term terrorism and demarcating the exact boundary between other illegal activities such as organized crime is also very difficult. Evidence shows that it is not enough to take account of the mere presence or absence of the primary political motivation in order to distinguish terrorist acts from criminal ones, but that the evaluation of the consequences of a terrorist act is an equally important criterion[17].

[15] M. Cejp, *Organised crime in the Czech Republic in 2006 compared with developments between 1993 and 2005*, Institute of Criminology and Social Prevention, Prague 2006.

[16] http://www.organized-crime.de/organizedcrimedefinitions.htm#fbi.

[17] D. Řehák, P. Foltin, R. Stojar, *Vybrané aspekty soudobého terorismu*, Ministerstvo obrany České republiky – AVIS, Praha 2008.

The above-mentioned "common criminals" may be used in the second group of "ideological" criminals, in which we include in particular political and religious terrorists in the context of this contribution, although they may be perpetrators with other motivations, but are always fanatics in their own right. However, the person who employs "common criminals" is the "ideological leader" of the terrorist group and has a different goal then they do. In this case, the role of "common criminals" is that of wage-earners, and their motive still consists in their own enrichment (however, they may in some cases also be coerced into cooperation).

The terrorist front includes a very diverse spectrum of attackers: from so-called lone wolves, through small groups, to military or paramilitary organizations, including the so-called Islamic State. The degree of connection varies, as terrorist groups have varied structures and forms of organization that emerge from the given group's operational conditions, traditions and possibilities, and structural changes thus occur in the course of their development. Most structural schemes of traditional terrorist groups are based on a unified general model. It can be portrayed as a pyramid with the staff and the hard core of the group at the top. It is a highly centralized structure for a terrorist organization that has been used mainly in the past[18]. It is what makes their structure similar to that of organized crime groups. However, today the relations and connections that allow for infiltration, ideological influence, and the dissemination of information, including instructions for the preparation and implementation of terror, have been greatly expanded due to information technologies (among other things). In some cases, it is still a defined (albeit decentralized) structure, and in some cases, the structure consists only of ideological successors from small groups and especially "lone wolves"[19]. This considerably hinders active defence by means of detecting and eliminating potential attackers before they attack.

Finally, it is worth mentioning attacks that have an external form of terrorism but are, in reality, attacks organized by a state. State terrorism includes attacks by hackers (allegedly, mostly from Russian and Chinese hackers, which have not been proven however), but (for purely technical reasons) we can also include the subcategory of active cyber-protection

[18] M. Brzybohatý, *Terorismus…*; Ministry of the Interior of the Czech Republic, http://www.mvcr.cz/clanek/definice-pojmu-terorismus.aspx.

[19] G. Weimann, *Lone Wolves in Cyberspace*, „Journal of Terrorism Research", 2012, no. 2.

of state interests through various computer tools, or cyberwarfare – see above. The most well-known example is the deployment of the Stuxnet virus[20], but this is far from being the only case.

Conclusion

In connection with the current trends in the area of information technology, such as the Internet of Things (IoT), Bring Your Own Device (BYOD), the transfer of data to clouds operated by third parties in various, often undefined, locations around the world, the massive collection and processing of personal data (by state and private entities), and the attempt to accelerate the use of artificial intelligence, it must be said that the more things become connected (i.e. become a part of cyberspace), the greater the risk of abuse that we have to anticipate will be. **The requirement of today is for all information and communication systems to be built as secure, regardless of their importance and scope**[21]**.** It can have unusual, or even fatal, consequences as a part of the fight against "ordinary" cybercrime on the one hand, but also against crime perpetrated by qualified and motivated perpetrators (cyberterrorists).

Despite the undoubted importance of prevention, which consists in building secure information systems, we cannot get by without considering means of strengthening the repressive side. In the medium to long term, it will likely be necessary to create entirely new external elements in the Criminal Code that affect forms of cyberattacks that are predicted despite their lower rates of occurrence hitherto while taking into account the high degree of societal dangers they pose due to their impact on the function of society.

References

1. Bastl M., *Kybernetický terorismus: studie nekonvenčních forem boje v kontextu soudobého válečnictví. Dissertation*, Masarykova univerzita v Brně, Brno 2007.
2. Brzybohatý M., *Terorismus I.*, Vydavatelství Police History, Praha 1999.

[20] V. Smejkal, *Kybernetická…*

[21] V. Smejkal, V. Porada, *Prevence jako účinná ochrana proti kybernetické kriminalitě*, [in:] *Zborník vedeckých prác z medzinárodnej konferencie BEZPEČNOSTNÉ FÓRUM 2017*, J. Ušiak, D. Kollár, M. Melková (ed.), Interpolis, Banská Bystrica 2017.

3. Cejp M., *Organised crime in the Czech Republic in 2006 compared with developments between 1993 and 2005*, Institute of Criminology and Social Prevention, Prague 2006.
4. *Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA)*, „Official Journal L", 22/06/2002, no. 164, p. 0003–0007.
5. *Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA)*, „Official Journal L", 22/06/2002, no. 164, p. 0003–0007, or § 311 of Act No. 40/2009 Coll., Penal Code, as amended.
6. http://www.organized-crime.de/organizedcrimedefinitions.htm#fbi.
7. https://www.europol.europa.eu.
8. Matoušková I., *Aplikovaná forenzní psychologie*, Grada Publishing, Praha 2013.
9. Ministry of the Interior of the Czech Republic, http://www.mvcr.cz/clanek/definice-pojmu-terorismus.aspx.
10. Netík K., Netíková D., Hájek S., *Psychologie v právu*, C. H. Beck, Praha 1997.
11. Řehák D., Foltin P., Stojar R., *Vybrané aspekty soudobého terorismu*, Ministerstvo obrany České republiky – AVIS, Praha 2008.
12. Schmid A. P., *Problémy s definováním terorismu,* [in:] *Encyklopedie světový terorismus. Od starověku až po útok na USA,* Svojtka & Co, Praha 2001.
13. Smejkal V. a kol., *Právo informačních a telekomunikačních systémů*, C. H. Beck, Praha 2004.
14. Smejkal V., *Kybernetická kriminalita*, Nakladatelství Aleš Čeněk, Plzeň 2015.
15. Smejkal V., Porada V., *Prevence jako účinná ochrana proti kybernetické kriminalitě*, [in:] *Zborník vedeckých prác z medzinárodnej konferencie BEZPEČNOSTNÉ FÓRUM 2017*, J. Ušiak, D. Kollár, M. Melková (ed.), Interpolis, Banská Bystrica 2017.
16. Smejkal V., Sokol T., Vlček M., *Počítačové právo,* C. H. Beck, Praha 1995.
17. Tafoya W. L., *Cyber Terror,* „FBI Law Enforcement Bulletin", November 2011, available at http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror.

18. *Tallinn manual on the international law applicable to cyber warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*, M. N. Schmitt (ed.), Cambridge University Press, Cambridge 2013.
19. Weimann G., *Cyberterrorism. How Real Is the Threat?*, „United States Institute of Peace, Special Report 119", December 2004. Available at http://www.usip.org/sites/default/files/sr119.pdf.
20. Weimann G., *Lone Wolves in Cyberspace*, „Journal of Terrorism Research", 2012, no. 2.

Cite this article as:

V. Smejkal, *From Terrorism to Cyberterrorism*, "Security Dimensions. International and National Studies", 2018, no 25, p. 118–130, DOI 10.24356/SD/25/6.