CRITICAL INFRASTRUCTURE PROTECTION (CIP) AS NEW SOFT TARGETS: PRIVATE SECURITY VS. COMMON SECURITY

Article *in* Journal of Security and Sustainability Issues · October 2020

DOI: 10.9770/jssi.2020.10.1(1)

CITATIONS
6

READS
276

2 authors:

Janos Besenyo
Óbuda University
185 PUBLICATIONS **406** CITATIONS
SEE PROFILE

Andras Istvan Feher
Óbudai Egyetem
3 PUBLICATIONS **6** CITATIONS
SEE PROFILE

JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2020 September Volume 10 Number 1
https://doi.org/10.9770/jssi.2020.10.1(1)

Scopus®

CRITICAL INFRASTRUCTURE PROTECTION (CIP) AS NEW SOFT TARGETS: PRIVATE SECURITY VS. COMMON SECURITY

János Besenyő[1], András Fehér[2]

[1,2]Óbudai *University, Doctoral School for Safety and Security Sciences, H-1081 Budapest, Népszínház utca 8., Hungary*

E-mail: [1]besenyo.janos@phd.uni-obuda.hu; [2]feher.andras@bgk.uni-obuda.hu

Received 15 February 2020; accepted 10 July 2020; published 30 September 2020

Abstract. 9/11 made terrorism a part of everyday life on a global basis, attacking civilisation as a whole. As a result, the activity of terrorist organisations reduces people's sense of security even in their everyday lives, by randomly attacking high public density targets with a huge emotional and publicity impact. The states cannot guarantee security through their law enforcement agencies alone, as the sources of danger have multiplied and become more unpredictable. Therefore, it is more important than ever to involve communities, social organisations, economic and market actors in maintaining common security. Private security thus plays by now an extremely important role in completing public order and security. The radicalisation trend within the terrorist organisations results in a growing number of internal terrorism threats. Given that terrorists aim to choose targets with a likely "success" of their acts, it is important to highlight those whose partial, temporary or total downtime entails consequences which would also make other infrastructures inoperative. Those who from these aspects turn to be the most important, and their continuous and well-functioning operation are essential to the operation of other infrastructures, are called critical infrastructures. If we put the above phenomena together, a clear conflict emerges: critical infrastructure protection, although in most cases not state owned, is also a common security issue, protected mostly by private security services, employing people mainly trained for private security tasks. Our article highlights this problem introducing the scientific background, also suggesting a possible solution for evaluation.

Keywords: terrorism; private security; common security; critical infrastructure; defence conflict

Reference to this paper should be made as follows: Besenyő, J., Fehér, A. 2020. Critical infrastructure protection (CIP) as new soft targets: private security vs. common security. *Journal of Security and Sustainability Issues,* 10(1), 5-18. https://doi.org/10.9770/jssi.2020.10.1(1)

JEL Classifications: Q10

1 Introduction

After the seventies, September 11, 2001 again made terrorism a part of everyday life, but this time on a global basis. The attacks on the Pentagon and the World Trade Center have made the world realise that the worldwide main threat is no longer the conflicts between countries, rather international terrorism. After 9/11 dozens of writings, analysis and expert explanations on terrorism emerged defining it as a new and major threat of the 21st century. By studying these, we can answer the following issues to help us understand terrorism:

- Investigation of the motive for terrorism.
- Investigation of state-sponsored terror and terrorist groups;
- Conceptual and substantive distinction between war and terrorism;

Before we examine these very closely, it is necessary to define the concept of terrorism. This is a rather difficult task though, having no uniformly accepted definition on one hand, while also realising that no matter how many formulations we look at, they all differ in many aspects. The main reason for this being that those formulating them look at the issue from different angles and thus naturally take different views.

The European Union defines terrorism as: "given their nature or context, may seriously damage a country or an international organization where committed with the aim of: seriously intimidating a population; or unduly compelling a Government or international organization to perform or abstain from performing any act; or seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization" (Gaertner 2003).

The United States has defined terrorism under the Federal Criminal Code, as: "...activities that involve violent... or life-threatening acts... that are a violation of the criminal laws of the United States or of any State and... appear to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and...(C) occur primarily within the territorial jurisdiction of the United States..." (Various Definitions of Terrorism).

According to Aviv Cohen, even the International Criminal Court (ICC) does not yet have jurisdiction over acts of terrorism as a distinct offense. The suggested provision defines the crime of terrorism as falling into one of the following three categories: "First, acts which constitute terrorism under a standalone definition that the provision provided; Second, an offense under six existing international counter terrorism conventions; or Third, offenses involving use of firearms, weapons, explosives, and dangerous substances when used as a means to perpetrate indiscriminate violence involving death or serious bodily injury to persons or groups of persons or populations or serious damage to property." (Cohen 2012).

Beyond the fact that we cannot provide even a uniform definition of terrorism, the actors also tend to evaluate the issue from their own, even radically different point of view.

However, after examining a number of terrorist acts, it can be seen that one of the common key elements is gaining publicity. This might be in many cases the only thing common in the various actions, regardless of the core motive. The aim is to inform the society about the action itself and the goals of the organisation, in order to influence the public and the governments by means of intimidation and insecurity, Thus, terrorist acts are created for and to influence the public. Without it, terrorism is mainly meaningless and pointless!

According to Catherine De Bolle, Europol's Executive Director, 'Terrorists not only aim to kill but also to divide our societies and spread hatred. That feeling of insecurity that terrorists try to create must be of the greatest concern to us. Increasing polarisation and the rise of extremist views is a concern for EU Member States and Europol.' (European Union 2019).

It is important to emphasize that the relativist concept of terrorism as 'one person's terrorist is another's freedom fighter' cannot be accepted! (Weinberg, Pedhazur & Hirsch-Hoefler 2004).

2 Security and Sense of Security

As an introduction to the topic, we need to clarify the categories mentioned in the title of the chapter, as they are not always clearly defined in the professional literature. It is our common scientific responsibility to use logical, clear and unambiguous terminology.

Security

As also seen regarding the phrase 'terrorism', we neither do have a commonly accepted security definition, although dozens of safety concepts are to be found in the literature. The first step to interpretation is to turn to etymology, namely to go back to the Latin form of the word security: securitas, -atis (f). The root of the word is cura, -ae (f), which means anxiety, fear, while 'se' means without. Combining the conceptual elements, we can conclude that the Latin term is used to express a state without fear or anxiety (WordSense.eu Dictionary).

In other words, the original meaning of the word security is that those are safe who are not in danger. What is important in this regard is that even if you do not face any real danger or risk, you may perceive a threat. Or the way around!

Despite that there are usually real reasons for the sense of danger, we must distinguish between the perceptual and the real side of security. Defining security as the absence of threat lets us differentiate between the objective and subjective dimensions of security. The subjective dimension of security may give rise to misjudgement of a situation or the development of unjustified fear. On one hand, we can evaluate how many threats people, societies and institutions actually face and what defence abilities they realistically have, and on the other hand, there is also a subjective perception of security (Baldwin 1997).

Security is a defining, fundamental category of security science, and it is clear from the above that security can only be interpreted in accordance with threat. Security is the combination of an existence or an activity and the factors that threaten it. Security and danger are a pair of categories, thus the term makes only real when a threat factor appears. The greater the risk to life or function, the lower the level of safety.

Security, in very simplified terms, is a state free from danger. From security science point of view, the endangered party is the existence of a person or the proper functioning of organisations, while the threatening party is an intentional unlawful conduct or act. Thus, from the point of view of security science, safety is a pairing of the existence of something or the proper functioning of something and the intentional unlawful conduct that threatens it (Smith & Brooks 2013).

The definition for personal and property protection is still incomplete, as we use defence resources to prevent it. Thus, personal and property protection is a changing dynamic state, which is directly influenced by two factors: the threat and the applied protection resources. The two factors work against each other: increasing the threat reduces the level of protection while the applied protection resources maintain or increase the level of security.

Thus, from a personal and property protection point of view, security is the interaction of the intentional unlawful conduct that threatens the life of somebody or the proper functioning of something and the protection resources applied against them. It is very important to underline the existence of intentionality and illegality concerning these acts, as in this very aspect, we exclude human inattention, neglect, catastrophes, etc. as hazards.

As seen, security is directly affected by the threat and the protection applied against it. A number of further factors affect security, like the legal environment, economic factors, the functioning of the insurance institution and security management systems, the state of the given public security, unemployment and corruption, among others (Buzan, Wæver & de Wilde 1998).

Safeguarding and Protection

The adequate place and role of safeguarding and protection is a huge issue regarding personal and property protection, that should be clarified. One of the questions is the professional relationship between safeguarding and protection. Are these two successive, supposing, or perhaps independent, coexistent categories?

Guarding is a countermeasure designed to prevent a likely, and to us unbeneficial or unnecessary activity (MacDonald 2009). Thus, guarding is basically a strictly regulated process of a tasks, commands and measures, presuming that somebody wants to take action against the guarded thing or person. At the same time, guarding has a demonstrative, deterrent role as well.

Protection is on the other hand the counteract of an intentional, unlawful conduct that is already taking place. Protection is thus an activity possibly to follow guarding, during which the unlawful activity is intentionally prevented or its consequences minimised.

Thus, guarding is a process linked to a hypothetical activity while protection is a response to a specific event already in action. In case of guarding, the time of the event, the number of offenders, their strength, their intention, their purpose, etc. are purely hypothetical contrary to protection where these are all specific (Schüller 2015).

Guarding is provided by the person on duty, possibly supported by technical equipment and/or guard dogs. In contrast, for protection, all available and enforceable means should be mobilised.

Complex Safeguarding

The complexity of guarding and protection is one of the defining problems of security services. In case of complex safeguarding, the applicable physical defence devices, electronic warning system and manpower should be determined following a relevant risk analysis and assessment, in order to achieve the desired level of protection.

The three forms of protection built upon and complementing each other gives the complexity. The perpetrator is in most cases confronted with a mechanical device when committing an illegal act, usually a kind of physical obstacle. To protect and monitor these mechanical instruments, various electrical sensing devices are. employed, which provide signal to the guards to let them decide on further steps to be taken.

Complex safeguarding should be effective. But what does this mean in practice? First, the budget spent on protection should be well balanced with the value of the object protection and its vulnerability. Moreover, the protection is expected to minimise the likelihood of a successful act while also maximise the risk for the perpetrator (of course, neither the likelihood can be zero, nor the risk 100%). Effectivity is when the proportions of all aspects are optimal (EU ESDP 2009).

Asset protection is thus complex and optimal if the use of mechanical instrument, electrical signalling devices and guards are proportionate to the protection task. The complexity of safeguarding also includes specific security policies and the information network required to operate the entire system.

Integrated Management System

Though not strictly part of our topic, we should devote some words to integrated surveillance systems, as these serve as the communication bridges between the different levels of complex safeguarding. An integrated management system is a system based on the integration of several types of hardware and software in order to receive, interpret, save, print, and acknowledge signals from the different devices.

3 Private Security and Common Security

Private security is a subset of security. With regard to security, it is now a common fact that in the era of globalisation, it is not possible to deal separately with external or internal threats within a society (Bigo 2006). The phenomenon of globalisation is a clear trend, despite counter tendencies also arising even most recently, so it is evident that the social context of the phenomenon has become the focus of interest among sociologists, criminologists, law enforcement professionals and researchers in the recent decades. The natural consequence of this trend is growing wealth disparities, among others, causing countless problems in social structures. Its direct relation to criminality has long been known as structural inequalities predict the spread of crime and violence (Irk 2012).

These thoughts sensitively highlight the consequence that state authorities assigned to common safety and security duties tend to be unable to solve the problem alone, calling private security into the game more than ever before.

One of the most decisive prerequisites for the widespread existence of private security services is the market itself, created by its even growing demand for security. Demand comes from wealthy individuals, legal entities, companies and businesses among others, moreover, also the states often appear in the client role.

However, it is very important to emphasise that private security do not have the same assets (in both legal and technical aspects) than those assigned to police and other authorities. The legal basis is mainly a civil law contract between the two parties for the private security sector.

The past two decades have shown, regardless if we look at our narrower environment or at global trends, that states cannot guarantee security through their law enforcement agencies alone. The challenges and sources of danger have multiplied and become more unpredictable. Therefore, it is more important than ever to involve citizens, their communities and other social organisations, economic and market actors in maintaining public security.

Private security plays by now an extremely important role in completing public order and security. We have already discussed above that private security actors "provide security" as a service. However, private security services now go far beyond protecting wealthy people and their wealth.

Private security companies (or often referred to as PSCs) are becoming increasingly important in our lives. In fact, new terminologies (e.g. public space) has emerged that blurs the sharp boundaries between public and private space, opening the door to private security providers (Krahmann & Friesendorf 2011). A significant part of the private spaces are also public space, where private security appears as a facilitator of common security.

It can be concluded from the above that the form and scope of the former classical services relating mostly to private real estate and private spaces is constantly expanding in line with the opportunities offered by the market. The security of the areas between public and private that intervene in our daily lives (e.g. shopping malls) also significantly influence the overall picture of public order and public security. That is why we can say that private security actors have not only a serious market opportunity, but also a proportionately serious responsibility, in terms of relevant crime rates and the development of citizens' sense of security. The importance of private security and its continuous expansion has become an indisputable fact nowadays.

The state controls and supervises private security and, in some cases, can interfere with the operation of it, and the it protects. For example, in order to protect private but otherwise high-risk facilities, businesses, goods of national value, natural values or land of public interest. Similarly, the state may impose on the economic operator or the interested party, as a condition of starting or continuing the business, mandatory rules of protection (for example: mass cultural events, sports facilities, gas stations, money changers, financial institutions, pawn shops, etc.). Due to the confidentiality of the private security services, the state shall determine the moral conditions, the material and legal requirements for the provision of these services, the training requirements and the examination procedure for service providers. In order to preserve the quality of its services and the order of fair economic competition, the state may, by economic and legal means, promote the establishment of an optimum balance between public and private interest in adequate protection (Kammersgaard 2019; Bilek, Klotter, & Federa 1981).

Private security firms have undoubtedly their place in this system, despite their distinctive features, and also because they represent the largest number of all those involved, regarding the number of their staff.

4 New World, New Enemy

The new type of terrorism no longer has any tangible purpose, it is attacking Western civilisation as a whole. The ETA, the IRA and other classical terrorist organisations in the second half of the 20th century fought for more or less specific goals, such as separation or independence of a territory. Today's Islamic terrorists, however, are attacking the Western world as a whole, and one of their main goals is to stir up disturbances and to

fuel conflicts between Europeans and Islamic immigrants. It is also important to distinguish between strong and radical solutions, and one of the goals of terrorists is precisely to radicalise the situation (Moghadam 2006).

After the disintegration of the bipolar world system, international terrorist organisations also became a part of the international system alongside the states. These terrorist organisations, like other international actors, act rationally, weighing the expected benefits and costs of their actions in order to achieve their goals as effectively as possible. The main purpose of the actors in the international system is to preserve or improve their position on the international stage and to ensure the viability of their future plans (Cooley 2012). This creates a competition in which international players aim for maximum performance. It is a spiral of violence in the relationship between terrorism and the states - in Korinek's words, an "irrational self-generating spiral" (Cohen 2012).

The efforts of the international actors to increase their own security result in a reduction in the sense of security of the opposite actor. All this entails a plethora of response back and forth.

The activity of terrorist organisations reduces people's sense of security, which encourages the states to increase their counterterrorism efforts. This, in turn, forces terrorists to use more advanced, increasingly destructive weapons: taking action only implies the need to take even more significant action in the future, which, without leaving the vicious circle, can trigger endless arms races. Terrorism researchers have pointed out that state measures to prevent the attacks also pose threat to democracies (The White House, Washington D.C. 2018).

Based on the above, strengthening state power in the fight against terrorism might not the best option. The other way around is if the state withdraws itself from the fight, which is also not considered the appropriate solution by researchers. According to Townshend, terrorists are playing on people's basic need and concern of sense of security and property. Fear and awareness of the inability of the state to protect its citizens from assassination, threatens the very existence of the state itself by the degradation of state authority and lost trust (Hudson 1999).

The army is an element of war, its application can only be conceived under those circumstances. However, terrorism has created a new kind of "war" conflict. It does not have a definite state or territory. Thus, on one hand, it does not have to comply with the rules of war to protect its citizens and residents, as is the case that characterises a conventional state, allowing it to fight with unlimited means. On the other hand, there is no exact front line where you can fight it – it is a new, "faceless" type of enemy! This also lengthens the fight, and the constant threat and lack of a separate, definable battlefield expands the front ground to the entire area of the threatened states.

It becomes inevitable to declare a kind of state of war, which may result in the permanent presence of the law enforcement forces and also excessive state dominance.

Terror sensitivity is the totality of the characteristics of persons and things that make them vulnerable to being relatively high risk victims of terrorist acts. A terrorist threat is a status, when a person, country, object, organisation is threatened by a terrorist organisation, but the terrorist act has not yet occurred.

Scientists who study the threat of terrorism and professionals who work with terrorist organisations recommend the adoption of three very important criteria when trying to define terrorism: (1) the use or threat of violence; (2) having a political motive or objective in the background of the attacks; (3) the threat of life or property of civilians during terrorist attacks (Khan 2006).

Nowadays, with the transformation of terrorism, the threat of terrorism is mainly the result of extremist Islamic terror groups, operating also outside the borders of Muslim religion.

The principle and practice of organising terrorist groups has also changed. Today, we are not just talking about international terrorism, but about a network of terrorist organisations. In a large terrorist organisation, we can speak of several sub-organisations that are either interdependent or independent (Shaw 2000). The tools and

methods used to commit terrorist acts have also changed. Terrorist groups use the internet widely to prepare for terrorist attacks and detonate more powerful explosive devices, yet the use of classical weapons also remained. Suicide bombings are a relatively new and serious challenge in the fight against terrorism. It is almost impossible to effectively protect against suicide bombers, either because the perpetrators significantly reduce the effectiveness of the most up-to-date detection systems by their self-sacrifice, or they can also change their target if they fail to execute their original plan (Besenyő 2017).

In the international literature and in the databases of scientific institutes and organisations dealing with terrorism, the targets of terrorist attacks are primarily registered based on the historical ones. In the various categories thus created, the basic ordering principle is when and where the target groups and objects have been attacked by terrorist organisations. The literature generally distinguishes terrorist attacks according to their target subjects: government, law enforcement agencies, diplomatic bodies, business interests, the media, transport system, tourism, energy and telecommunications systems, educational institutions and religious communities.
According to the areas of attacks and threats, a distinction should be made as follows:

- Rural attacks;
- Urban attacks;
- Attacks in the cyberspace.

With a few exceptions, terrorist acts in rural areas were characterised by a low number of victims, despite the fact that they were primarily aimed at transport structures and vehicles. However, their impact often went beyond the location of the terrorist attack and its environment, sometimes due to the nature of the transport network, regardless of the amount of material damage (Hoffman 2006).

The danger of terrorist threats to energy supply systems and public utility networks has already been pointed at by professionals. Al-Qaeda's leader, Osama bin Laden, had already threatened in December 2004 with the destruction of Saudi oil plants. In recent years, energy supply systems and terrorist attacks on oil facilities, oil and gas pipelines have increased in India, Pakistan and Saudi Arabia. Or most recently, on March 31th, 2020, an explosion damaged and halted flow of a natural gas pipeline in eastern Turkey, in the town of Dogubayazit, most possibly attacked by Kurdish militants. The terrorist threat of energy and utility networks also extends beyond local areas: a terrorist attack may have a direct or indirect impact on a regional basis or even at a global level, threatening the personal and financial security of millions and possibly hindering the access to vital energy sources (National Research Council of the National Academies 2012).

Metropolitan areas have advanced public utility, transport and telecommunications networks to serve the residents and to provide infrastructure, facilities and operating conditions for institutional systems. These networks are complex and vulnerable systems, so protecting them from terrorist attacks is a very expensive and almost impossible task. In addition to the high population density, the relatively easy vulnerability of infrastructure and networks increases the vulnerability of large cities to terrorist attacks. Terrorist organisations also benefit from the network nature of public utilities, urban public transport and IT systems, since the effects of the attacks are not only felt directly at the locations but far beyond as well (Görbe 2010).

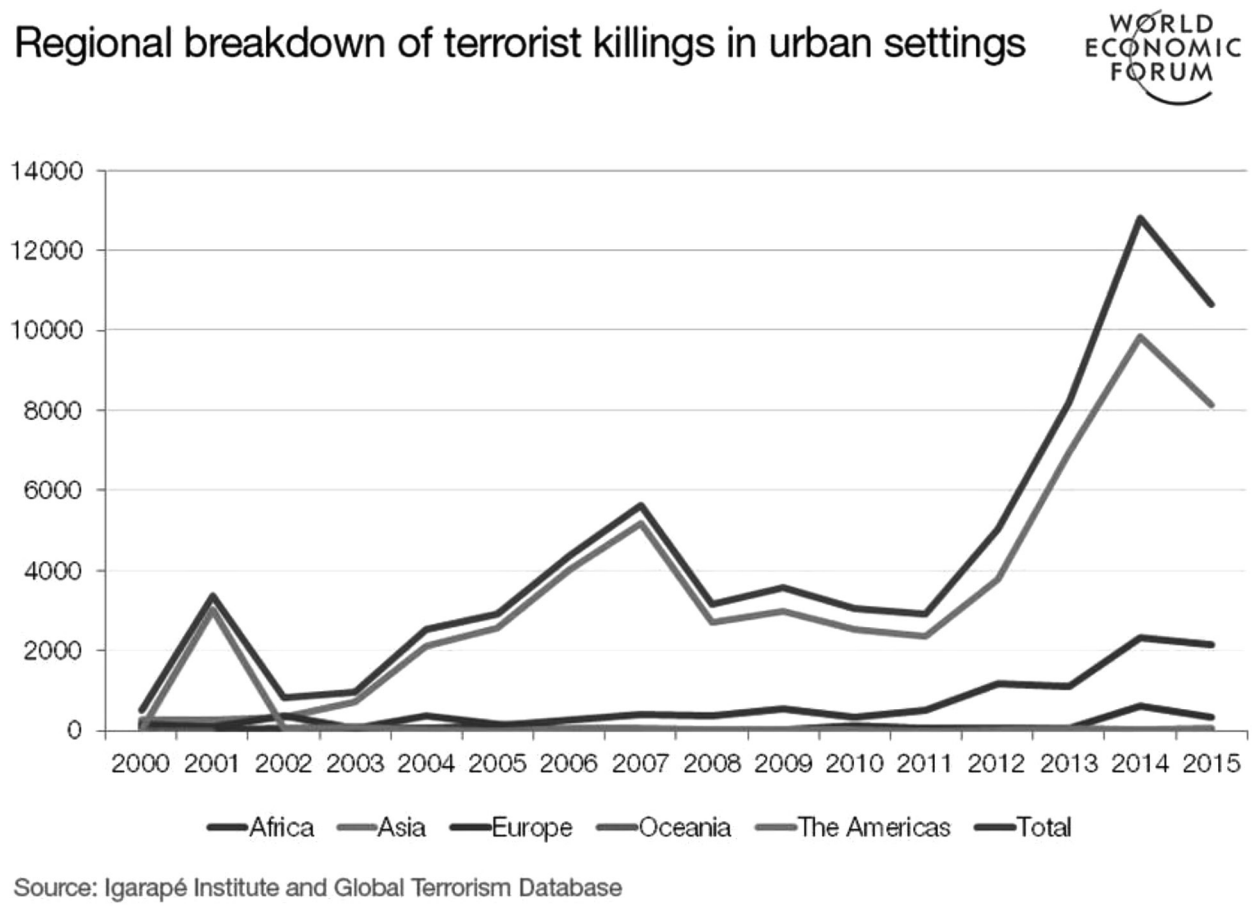

Figure 2. Regional Breakdown of Terrorist Killings in Urban Settings

Source: Robert Muggah, Katherine Aguirre: "Terrorists want to destroy our cities. We can't let them", World Economic Forum, 2016, Retrieved from: https://www.weforum.org/agenda/2016/12/terrorists-want-to-destroy-our-cities-we-can-t-let-them/

The incredible degree of technical development also favours terrorists, as today, not only them, but also an IT professional with above average capabilities are capable of developing software that could pose potential threats to the public administration, energy, banking, utilities, transportation services, and more (Adomi 2011). If terrorists start to use the tools and methods of cybercrime in large, Western countries will have to face new challenges. The stake in this case would be the access to the achievements of civilisation and technological development.

Several types of groupings based on the selection of targets by the terrorist organisation are also used in the international terrorism-related repositories. According to the above, the basic aspect of grouping is the identification of objects of the endangered target group. As there is a radicalisation trend within the international terrorist organisations, this grouping should be supplemented by the guiding principle of what the motive of selecting the targets can be. Furthermore, analysing target selection is also interesting in order to show the direction in which terrorist groups' violence are moving (Böröcz 2015).

On this basis, the following grouping is proposed:

- Relatively predictable victims or target victims;
- A group of victims and targets selected almost entirely randomly (Sarah Max Research 2017).

Those terrorist attacks which are of the latter category, are mainly carried out in shopping malls, cultural and sporting facilities, restaurants, entertainment venues, museums, public transport and places favoured by tourists. The radicalised terrorist organisations, decreasingly selective in their means and methods, can go for sure

regarding the likely "success" of their acts, as it is most sure to find masses at the targeted places at certain times of the day. This is one of the reasons why urban public transport vehicles and facilities have become a popular target for terrorism. Analysing the growing number of terrorist acts claiming almost entirely randomly selected victims, it has been found that in recent years, the majority of victims of terrorism have died or been seriously injured because they were accidentally present in a place where the act occurred (Riley 2014).

5 Critical Infrastructures

Infrastructure is defined as the set of systems, or elements thereof, that ensure the proper functioning of the given organisation. There are numerous infrastructures that can be distinguished by their importance, function, purpose and structure. Of these, however, it is important to highlight those whose partial, temporary or total downtime entails consequences which would also make other infrastructures inoperative. Those who from these aspects turn to be the most important, the most vulnerable, and their continuous and well-functioning operation are essential to the operation of other infrastructures are called critical infrastructures (Green Paper on an European programme for critical infrastructure protection 2005).

Going from security to terrorism, it might not come as a surprise that there are several definitions of critical infrastructure as well, although with very similar content. The security issues, assessed differently from country to country, further complicate the precise definition of critical infrastructure and the process of interpreting criticality itself.

The existence of national institutions linked to critical infrastructure protection in Western countries makes it clear that developed countries have already developed their own criteria upon which to select the infrastructures to be classified as critical.

The (US) President's Commission on Critical Infrastructure Protection (PCCIP) issued a report in October 1997 which identified five critical infrastructures: "energy, banking and finance, transportation, vital human services, and telecommunications--that are essential to national defense, public safety, economic prosperity, and quality of life. (…) However, the widespread use and interlinkage of computer and telecommunications throughout these infrastructures has created new vulnerabilities which, if not addressed, pose significant risks to our national security." (US Senate Select Committee on Intelligence 1998).

NATO's Senior Civil Emergency Planning Committee (SCEPC) began developing policies on critical infrastructure protection in 2001, primarily through the exchange of experience, research and assessment processes, and international cooperation. According to NATO's approach critical infrastructure protection, besides prevailing the related military requirements, should focus on protecting the population, maintaining the economy, providing civilian assistance in military situations and military engagement in civilian tasks. Accordingly, in a directive adopted in 2003, NATO also created its own concept of critical infrastructure, which is "facilities, services, and information systems that are vital to nations so that their failure or destruction would have a detrimental effect on national security. National Economy, Public Health, Public Security and the Effective Functioning of Government " (Based on the Critical Infrastructure Protection Concept Paper 2003).

In recent years, within NATO, research activities have been conducted to map dependencies, develop Civil-Military Cooperation (CIMIC) capabilities, establish the theoretical aspects of risk management and to provide the necessary expertise (North Atlantic Treaty Organization 2011).

Given its union nature, the concept of critical infrastructure in the European Union is more detailed, explicitly aimed at the unity of the Union, but still not very specific. The Green Paper defines "physical assets, services, information technology facilities, networks and assets" as critical infrastructures "the disruption or destruction of which would have serious consequences for the health, peace, security or economic well-being of Europeans, or for the effective functioning of the EU and the governments of its Member States." (Based on the Green Paper of the European Union 2005) Some of these critical infrastructures are (European Parliament recommendation

to the European Council and to the Council on the protection of critical infrastructure in the framework of the fight against terrorism 2005):

- Energy production, storage and transport infrastructures: coal and oil fired, gas, hydro, wind, solar, biogas and nuclear power plants, natural gas and oil production and refineries, coal mines, electricity converters, power lines, oil - and natural gas pipelines, etc.
- Banking and financial infrastructures: banking networks, shopping centres, value and commodity exchanges, other financial organisations;
- Water supply systems: water purifiers, reservoirs, plumbing and drainage systems, etc.
- Telecommunications and communication systems: telecommunication and communication equipment, which include computer-based networks, software, etc.
- Transport infrastructures: national airlines, airports, road passenger and freight transport companies, road and motorway networks, railway companies, rail networks, water transport equipment, etc.
- Emergency and civil protection infrastructure: emergency services, police, fire brigade, health institutes, disaster recovery services, etc.
- Governmental and municipal bodies.

It is clear from this list that, although they are separate systems, they are very often related. For example, energy supply is a prerequisite for the functioning of many other, very important, also critical infrastructures. Consequently, even if we do not aim to prioritise any of the listed infrastructures, we can safely say that the partial or total failure of power supply systems for a longer or shorter period of time can have a serious impact on other infrastructures (Proposal for a Council Decision on a Critical Infrastructure Warning Information Network 2008; Robert, Morabito, Cloutier & Hémond 2013; Fialka 2016; Plėta, Tvaronavičienė, & Della Casa, 2020).

6 Defence Conflict

If we put the above phenomena together, a clear conflict emerges: critical infrastructure protection, although in most cases not state owned, is also a public security issue, protected mostly by private security services, employing people mainly trained for private security tasks.

Challenge

Epitomising the previous chapters, we face the following challenge:

- The borderline between public and private security is fading;
- Terrorism is radicalising, targets are often selected randomly;
- We now can speak of several sub-organisations, rather than only centralised groups of terrorists;
- Terrorist acts created for and to influence the public: stir up disturbance and feeling of insecurity among people;
- The network nature of Western public utilities, urban public transport and IT systems and their growing number and dependence on them;
- Increasing number of suicide bombings and actions: new type of “faceless” enemy, living among us, no common recognisance: neither age, sex or nationality;
- Immigrant crisis Europe;
- Cybercrime also being a growing threat;
- A kind of non-official permanent state of war parallel with an official state of peace.

If we add, that the most common key elements behind the attacks is gaining publicity, it is easy to see that critical infrastructures in the developed countries are possible targets, protected by differently trained and not combat ready civilians.

Most of the recent attacks were performed by residents of the same country where the incident took place. Moreover, taking an example from aviation terrorism, where we see a clear tendency that terrorist organisations now prefer to recruit aviation employees for the attacks who have access to the restricted areas within the airports, the same method might be applied against other critical infrastructures as well (Townsend & Beaumont 2015). Thus, the front ground may rea+lly expand to the entire area of the threatened states.

Possible Solution

The way to go is basically a tripartite approach:

- Counter-terrorism: either by steering international politics towards peace or compromise with the organisations or fight them;
- To strengthen the intelligence agencies and system for early and more effective reconnaissance;
- Antiterrorism: to improve the security level of critical infrastructures, especially those that also serve other ones.

The first two options are not related to our topic, but the latter is.

Despite having concluded that strengthening state power in the fight against terrorism might not the best option, it can be the best there is, in some cases. Security is mostly a reactive profession: we give answers to threats and incidents to prevent further ones. Think of for example the Brit Richard Reid, who on December 22, 2001 intended to detonate a bomb built in the heels of his shoes on a flight from Paris to Miami. He was caught, but we bear the consequences of this in the airport Transportation Security Administration (TSA) protocol ever since (Craig 2001).

As we saw, the world is changing: we face new enemy images, sometimes even new enemies, who are searching for new targets. These demand new approaches from our side as well, and we need to take control rather than being reactive, as also taking the radicalisation tendency into consideration, the impact of a possible attack might be enormous thus inadmissible.

On an administrative and legal level, protocols and laws should be entered into force to improve the security levels of the cited infrastructures, while also on a practical ground it should be stated that the private security companies also serve public security interests.

This latter needs paradigm shifts in most countries and rises a lot of questions to be answered, among them:

- The legal relation between private and public security: its place in the line, supervisory bodies etc.
- Private security company topics: licences, education, trainings, responsibilities etc.
- Mobilisation in emergency situation;
- Reliability matters, both safety and security;

These are truly invasive issues to find the right answers for by all means, but maybe it is time to be proactive and regain control: we would sacrifice a bit of convenience on security's altar, but be able to protect our citizens and infrastructure and also our democratic institutions on the other hand.

Conclusions

The aim of our work is to reflect on the difficulties of antiterrorism fight. We have tried to highlight the points that illustrate the main contradictions in this fight. After defining the expressions and their backgrounds, we have shown what challenges today's tendencies in terrorism radicalisation might bring for the near future.

After September 11, the world's attention turned to the United States. Counter-terrorism measures have taken

a new direction, creating a more offensive approach. However, the question arises as to whether the countries have chosen the appropriate course of action.

Strengthening state power in the fight against terrorism might not the best option. This also lengthens the fight, and the constant threat and lack of a separate, definable battlefield expands the front ground to the entire area of the threatened states, unavoidably declaring a kind of state of war.

We have highlighted the current situation to show that critical infrastructures are on the battlefield of the fight against terrorism. Although it is not happening widely yet, we cannot ignore the fact that due to its privileged status, critical infrastructures have come within the horizons of terrorism.

This, supplemented with the fact that these infrastructures tend to be guarded by PSCs leading to a clear conflict situation between the primarily aim of private security and the role it also has to play, urges for unified international concepts and best practises.

This is not easy though, due to different state interests, resulting in terrorism taking advantage of this situation, which is why it is emerging with increasing force.

In our view, it is a priority to consider these dangers and develop a position that is appropriate to the majority of states, before the increasingly devastating terrorist attacks sweep societies into a hopeless situation. In the meantime, we have to adopt to the circumstances and find a way to protect our culture and the achievements and technological development of civilisation.

References

Adomi, E. E. (2011). Handbook of research on information communication technology policy: Trends, issues and advancements. Scopus. EISBN 13: 9781615208487.

Baldwin, D. (1997). The concept of security. *Review of International Studies,* 23(1), 5–26. Retrieved from: www.princeton.edu/~dbaldwin/selected%20articles/Baldwin%20(1997)%20The%20Concept%20of%20Security.pdf

Based on the Critical Infrastructure Protection Concept Paper EAPC (SCEPC) D (2003). 15 formulated by the NATO Committee on Civil Protection.

Based on the Green Paper of the European Union (Green Paper on a European Program for Critical Infrastructure Protection - COM (2005) 576 final

Besenyő, J. (2017). Low-cost attacks, unnoticeable plots? Overview on the economical character of current terrorism. *Strategic Impact* (1/2017), ISSN 2029-7017.

Bigo, D. (2006). Internal and external aspects of security. *European Security*, 15(4), 385-404. https://doi.org/10.1080/09662830701305831

Bilek, A. J., Klotter, J. C. & Federa, R. K. (1981). Legal aspects of private security. *Anderson Pub. Co.*

Böröcz, M. (2015). Investigating the relationship between illegal migration and terrorism. *Budapest: Counter-Terrorism Center*

Buzan, B., Wæver, O. & de Wilde, J. (1998). Security: A new framework for analysis. *Boulder (US-CO)*, Lynne Rienner Publisher.

Cohen, A. (2012). Prosecuting terrorists at the international criminal court: reevaluating an unused legal tool to combat terrorism. *Michigan State International Law Review*. Retrieved from: https://digitalcommons.law.msu.edu/cgi/viewcontent.cgi?article=1080&context=ilr

Cooley, A. (2012). Great games, local rules. *New York, Oxford University Press Inc.*, ISBN 978-0-19-992982-5

Craig, O. (2001). From tearaway to terrorist - The story of Richard Reid. *The Telegraph* (December 30, 2001), Retrieved from: https://www.telegraph.co.uk/news/uknews/1366666/From-tearaway-to-terrorist-The-story-of-Richard-Reid.html

EU ESDP (2009). European security and defence policy: the civilian aspects of crisis management. Retrieved from: www.zifberlin.org/fileadmin/uploads/analyse/dokumente/EU_ESDP_Civilian_aspects_of_crisis_management_-_version_3_EN.pdf

European Parliament recommendation to the European Council and to the Council on the protection of critical infrastructure in the framework of the fight against terrorism (2005/2044(INI)), Retrieved from: https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52005IP0221&from=HU

European Union. (2019). Terrorism situation and trend report. *Europol*, ISBN 978-92-95209-76-3. https://doi.org/10.2813/788404

Fialka, Gy. (2016). The concept, origin, present, future of financial institution security, conditions and significance of paradigm shift. *Doctoral (PhD) Dissertation, Budapest: Óbuda University, Doctoral School of Security Sciences*.

Gaertner, H. (2003). European Security: The End of Territorial Defense. *The Brown Journal of World Affairs,* 9(2), 135-147.

Görbe K. Z. (2010). The migration situation in Hungary, conditions and possibilities for its management. *PhD dissertation, Budapest: Miklós Zrinyi National Defense University*.

Green Paper on an European programme for critical infrastructure protection – COM (2005) 576 final

Hoffman, B. (2006). Inside terrorism. *New York: Columbia University Press*.

Hudson, R. A. (1999). The sociology and psychology of terrorism: who becomes a terrorist and why?. *Library of Congress*, Retrieved from: https://fas.org/irp/threat/frd.html

Irk, F. (2012). Doubtful criminology. *Magenta Publisher*, Miskolc

Kammersgaard, T. (2019). Private security guards policing public space: using soft power in place of legal authority. *Policing and Society Journal*

Khan, A. (2006). The theory of international terrorism. *Connecticut Law Review*, Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=935347

Krahmann, E. & Friesendorf, C. (2011). The role of private security companies (PSCs) in CSDP missions and operations. Retrieved from: https://www.researchgate.net/publication/332849133_The_role_of_private_security_companies_PSCs_in_CSDP_missions_and_operations

MacDonald, D. (2009). Safeguarding adults - theory into practice. *The Journal of Adult Protection*, 11(2), 42-48. https://doi.org/10.1108/14668203200900014

Moghadam, A. (2006). Suicide terrorism, occupation, and the globalization of martyrdom: a critique of dying to win. *Studies in Conflict & Terrorism*, 29(8), 707-729. https://doi.org/10.1080/10576100600561907

Muggah, R. & Aguirre, K. (2016). Terrorists want to destroy our cities. We can't let them. *World Economic Forum*. Retrieved from: https://www.weforum.org/agenda/2016/12/terrorists-want-to-destroy-our-cities-we-can-t-let-them/

National Research Council of the National Academies. (2012). Terrorism and the electric power delivery system. *The National Academies Press*, ISBN 13: 978-0-309-11404-2

North Atlantic Treaty Organization (2011). Civil-Military Cooperation (CIMIC). Retrieved from: https://www.nato.int/cps/en/natohq/topics_69722.htm

Peto, R. & Tokody, D. (2019). Building and operating a smart city. *Interdisciplinary description of complex systems - Scientific Journal*, 17(3-A), 476-484. http://indecs.eu

Plėta, T., Tvaronavičienė, M., & Della Casa, S. (2020). Cyber effect and security management aspects in critical energy infrastructures. *Insights into Regional Development*, 2(2), 538-548. https://doi.org/10.9770/IRD.2020.2.2(3)

Proposal for a Council Decision on a Critical Infrastructure Warning Information Network – CIWIN (COM(2008) 676 final), Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52008PC0676&from=EN

Riley, J. (2014). Terrorism and rail security. *RAND.* Retrieved from: http://www.rand.org/content/dam/rand/pubs/testimonies/2005/RAND_CT224.pdf

Robert, B., Morabito, L., Cloutier, I. & Hémond Y. (2013). Interdependent critical infrastructures: from protection towards resilience, Retrieved from: https://www.emerald.com/insight/content/doi/10.1108/DPM-10-2013-0195/full/html

Sarah Max Research (2017). No-go areas: American and European ghettos of broken dreams. Retrieved from: https://sarahmaxresearch.com/2017/03/29/no-go-areasamerican-and-european-ghettos-of-broken-dreams/

Schüller, A. (2015). Examining the human factor in the fields of information security, body guarding and property protection and evacuation. *PhD Dissertation, National University of Public Service, Doctoral School of Military Engineering* https://doi.org/10.17625/NKE.2016.09

Shaw, M. (2000). The development of "common-risk" society: theoretical overview. Kuhlmann, J. – Callaghan, J. M. (eds.) *Military and Society in 21*st *Century Europe. A Comparative Analysis.* New Brunswick (US-NJ) – Hamburg, Transaction Publishers – LIT Verlag

Smith, C. L. & Brooks D. J. (2013). Security science: the theory and practice of security. *Butterworth-Heinemann*, https://doi.org/10.1016/C2011-0-06978-8

The White House, Washington D.C. (2018). National strategy of countering weapons of mass destruction terrorism. Retrieved from: https://www.whitehouse.gov/wp-content/uploads/2018/12/20181210_National-Strategy-for-Countering-WMD-Terrorism.pdf

Townsend, M. & Beaumont, P. (2015). Russian plane crash: Calls for new era of airport security after Sinai terror. *The Guardian* (November 8, 2015), Retrieved from: https://www.theguardian.com/world/2015/nov/07/new-era-airport-security-sinai-terror

US Senate Select Committee on Intelligence (1998) Overview of the senate select committee on intelligence responsibilities and activities. Retrieved from: https://www.intelligence.senate.gov/publications/report-accompany-s-2052-intelligence-authorization-act-fiscal-year-1999-may-7-1998

Various Definitions of Terrorism. Retrieved from: https://dema.az.gov/sites/default/files/Publications/AR-Terrorism%20Definitions-BORUNDA.pdf

Weinberg, L., Pedhazur, A. & Hirsch-Hoefler, S. (2004). The challenges of conceptualizing terrorism. *Terrorism and Policical Violence*, 16(4), 777-794. https://doi.org/10.1080/095465590899768

WordSense.eu Dictionary, Retrieved from: https://www.wordsense.eu/securitas/

János BESENYŐ
ORCID ID: http://orcid.org/0000-0001-7198-9328

András FEHÉR
ORCID ID: https://orcid.org/0000-0002-5130-1693