DOI: 10.38146/BSZ.SPEC.2020.2.6

Gabriella Ráczkevy-Deák

Hospital Security: Hospitals and Terrorism

Abstract
Hospitals are part of the critical infrastructure and are incredibly vulnerable. Unexpected events may hinder the functioning of institutions, causing severe damage and loss of asset value and quality of service. Every hospital should be prepared for such incidents with well-developed plans and strategies. A hospital can be an ideal target for a terrorist, because a lot of civilians are taken care of (and are open) 24 hours a day, seven days a week. Unfortunately, in recent years have taken place more and more terrorist acts. (eg: 13th November 2015 Paris, and 22nd March 2016., Brussels). How are hospitals prepared for these events in Hungary and abroad? Are the Hospitals Disaster Management Plans sufficient? What kind of terrorist attacks can occur in a hospital (e.g. cyber terrorism)? In my essay I am looking for the answers to these questions and introducing the concept of hospital safety and security.

Keywords: hospital, security, soft target, terrorism, critical infrastructure

Introduction

Hospitals are part of the critical infrastructure and are incredibly vulnerable. Unexpected events may hinder the functioning of institutions, causing severe damage and loss of asset value and quality of service. Every hospital should be prepared for such incidents with well-developed plans and strategies. In this article, I am looking for an answer about how the hospitals in Hungary, in Western countries, and in the USA are prepared for these disasters and impacts resulting from human reactions towards these acts of terrorism. Is it possible to eliminate harmful effects of these events thought adequate preparations? An organization that is prepared for unexpected events can reduce damage. How can be a conscious institute leader prepared for preventive actions? A hospital

can be an ideal target for a terrorist attack, because a lot of civilians are taken care of and is open 24 hours a day, seven days a week.

Critical infrastructure conception

According to the Green Paper on a European Programme for Critical Infrastructure Protection the critical infrastructure is composed of device systems, or parts of systems which can be found on the territory of member states and which are essential for providing the vital social functions, health, and security, economic and social welfare. (URL1) The disruption or destruction of any of these device systems, or parts of systems could lead to important consequences due to the lack of supplying the vital functions.

The Green Paper divides the critical infrastructure in nine different groups:

1.) Energy facilities and networks
2.) Communications and Information Technology
3.) Finance
4.) Health care (hospitals, health care and blood supply facilities, laboratories and pharmaceuticals, search and rescue, emergency services)
5.) Food
6.) Water supply
7.) Transport
8.) Production storage and transport of hazardous materials
9.) State Infrastructure

The European Union Critical Infrastructure Protection Program (EPCIP) adjusted the interruption or loss of the infrastructural functioning to the size and severity of the possible consequence. Hungary has created and adopted the National Green Paper (NGP-NKIV) by Government Resolution. NGP lists the possible dangers into three main groups, taking the priority of terrorism as a basic principle. It highlights the *'acts of terrorism and its instruments, and related acts (explosives, misuse of firearms…).'* (URL2) The Green Paper emphasises the need for an appropriate security level in order to reduce risks to an acceptable minimum level. It also emphasises paying attention to communication and effectuating regular trainings because it makes the implementation of the plans more effective. The experience and information transfer between agencies, regions, and countries is also very important in prevention.

How can we define the concept of terrorism?

There is no clear definition for terrorism. Terrorism is defined in several ways by organizations. According to United States Federal Bureau of Investigation (FBI), the terrorism is the unlawful use of force or violence against people or property, the intimidation of the government, the civil population or any segment and coercion for political purposes and to promote social goals. (URL3) The UN says: *'crimes which aim with a political purpose to arise terror in the general public, group of people, or in individuals*(...)*'* (URL4) Terrorism uses violence for the purpose of achieving socio-political goals through fear. So, they struggle to achieve their goals by violent means (explosion, armed violence, etc.). Generally, terrorists are committed to more violent acts doing this in a pre-planned manner (Tálas, 2006, 66.). A very important peculiarity is creating panic-fear and victims. However, it is important to distinguish terrorists from ordinary criminals. Motivations and goals are different. Anyone who wants to acquire property, or injuries people because of offences, acts because of selfish reasons, it wants to achieve no psychological effect. He does not convey any message for the State Government and does not want to influence public opinion. The insane bomber mainly takes somebody hostage or shoots because of personal reasons. The terrorists have political intentions and want to achieve a violent and psychological effect and may have an organization in the background (Besenyő, 2016. 5.). Their aim is to spread terror to influence society by mains of that. The person who threatens with bomb, usually has personal reasons to create panic so that I would describe him as an ordinary criminal but not as a terrorist.

Figure 1. Terrorist targeting objectives (by Hospitals. Potential indicators of terrorist activity, common vulnerabilities and protective measures 2007. (URL6)

The explosion in one of the most commonly used instruments of terror, induces a great panic, has a significant, spectacular impact and it is difficult to prevent. However, each institution must expect and be prepared for such situations. A bomb threat is designed to create panic. Every public danger (bomb) threat call has to be taken seriously and should be treated as if it were true (Pascal, 1977, 111). The vulnerability of the institution is real and requires constant readiness. These calls may be very common, and their motivation is to enforce or cause malfunction. The special method of defence shall be determined according to the nature of the received information.

Hospital safety and security

A lot of people, and security teams too, use these two expressions safety and security as synonym words. But they are not synonym. Safety is the prevention of accidents, not intentional cases, security is the prevention of malicious activities by people like robbery, terrorist activities etc. The safety and security can be defined as a system, having the task to protect the property of the institute as well as to provide a relative protection of all persons who interact with the institution and its environment. Security is not a static concept; it can be viewed as a fluctuating state or situation. As the environment and human circumstances change, so changes the protection status. These factors could be divided into three groups: the assets and rights of staff, patients' rights and valuables, as well as the risk factors affecting the operation of the hospital (Besenyő – Deák, 2010, 19.)

Some studies divide the hospital security threats in interior and exterior group. Harmful factors for hospitals can be divided into their origin and development:

1. external threats, such as natural disasters, terrorism, demonstrations, etc.
2. internal hazards. These are the factors that result from the operation and the health activities (Pascal, 1977, 111.).

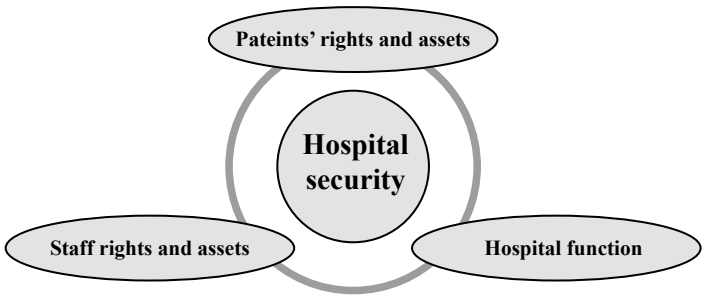

Figure 2. Hospital security threats (made by the author.)

Hospitals as soft targets

What does soft target mean? Soft Targets:

- Persons or things relatively unprotected or vulnerable, especially to a military or terrorist attack.
- More attractive to terrorists (significant casualties, economic/psychological). (URL5)

While there are many other soft targets, such as schools, sporting arenas, amusement parks, and theatres, hospitals have relatively unique vulnerabilities. Unlike other soft targets, hospital patients are often very sick or otherwise disabled, unable to ambulate, and hard to evacuate from a menacing situation damage (Fiuncane, 2017, 6.).

Hospitals have common vulnerabilities:

Visibility, accessibility and population: open to public with multiple entrances, metal detectors are rarely present, easy access by motorized vehicles, including parking close to hospital, potential for mass casualties, diverse staff, and lack of background checks. Presence of hazardous, toxic, and explosive materials: potential to spread dangerous chemicals, microbes, or radionuclides through the ventilation system, potential for explosions and fire, such as liquid fuel, or gasses or medical gases, attractive theft targets such as radionuclides and pharmaceuticals, unprotected, easily accessible utility supplies (URL6). Hospitals, and the Emergency Departments in particular, are vulnerable and are real soft targets for terrorists aiming to destabilize society. Historically, one would think that one's hospital would not be targeted by international or domestic terrorists. Two researchers reviewed worldwide terrorist attacks on hospitals in the period 1981-2013 and collected data of approximately 100 attacks, altogether resulting in 775 casualties in 43 countries. They concluded that many health care workers have already been confronted with terrorism as a victim. The motives of the terrorists were diverse, ranging from ideas derived from nationalistic to communist to Islamic beliefs (Cauwer – Somville – Sabbe - Mortelmans, 2016, 99.). Not only do government authorities consider the medical and emergency sectors to be capital targets, both domestic and international terrorists also consider these sectors to be possible targets.

Terror acts against hospitals

I cannot discuss this topic without pointing out that I write about a very real problem even if experts consider terrorism only as a potential threat in Hun-

gary. In our country a bomb threat against hospitals is more likely to occur. In the following chapter I present some terrorist attacks against foreign hospitals.

14/06/1995 Chechnya

In the bloodiest years of the Chechen war an attack took place near the border of Chechnya. On 14th June 1995 Chechen armed forces occupied the whole city of Budyonnovsk. Almost 1500 civilian hostages were taken by the militants led by Shamil Basaev. The hostages were detained for six months in the hospital and city health care. After six-months of awaiting the Russian troops besieged the city and the hospital. 129 people died and 500 people were wounded in the attack. 18 of them died later due to injuries (URL7).

2/08/2003 Mozdok

On the evening 02.08 2003. in Mozdok belonging to the Northern Ossetian Land (Russia), two suicide bombers draw a track loaded with explosives against a military hospital. The detonation of 100 kg TNT destroyed the building completely. In the explosion 42 people were killed and 78 were injured (URL8).

04/11/2005 Iraq

In Iraq, a bomb killed 30 people in a hospital courtyard. Because of the good security system, the bomber was not able to get into the hospital (URL9).

16/04/2010 Pakistan

At least eight people were killed, and 35 people injured in a bomb blast, which occurred in a hospital in the south-western Pakistani city of Quetta. Gunfire could be heard after the explosion of the civil hospital. Two policemen and a local television cameraman were among the casualties. The bomber detonated the explosives-filled jacket (URL10).

06/08/2010 Istanbul

In Istanbul, a bomb exploded in front of a hospital, precisely at the arrival of the police. 15 people were injured (URL11).

06/01/2010 Pakistan: Lahore

Five people, including three policemen were shot when four bombers wearing police uniforms rushed into the Jinnah Hospital's emergency department late in the evening. They wanted to save or kill a fellow patient who was injured in another attack. The bombers could not be apprehended they escaped (URL12).

Cyber-attacks:

05/2017 United Kingdom's National Health Service worm

WannaCry attack on the UK National Health Service (NHS) in May 2017. The UK National Audit Office reports: The attack led to a disruption of at least 34% of trusts in England although the Department and NHS England do not know the full extent of the disruption. On 12th May, National Health Service England initially identified 45 NHS organizations including 37 trusts that had been infected by the WannaCry ransomware. Over the following days, more organizations reported they had been affected. In total, at least 81 out of 236 trusts across England were affected (URL13).

01/2018 hackers had breached Norway's IT system of hospital

An incident in Norway illustrates that cyber espionage against the healthcare sector is a reality. In January 2018, it was revealed that hackers had breached an IT system at a hospital (URL14).

Attacks' consequences

Attacks on hospitals also could cause long-term effects: hospital units could be unavailable for a long time and replacing the staff could take several months, further complicating hospital operations. Both physical and psychological (e.g. posttraumatic stress disorder (PTSD) after-effects of a terrorist attack can be detrimental to health care services are most of the time civilians (Harald et.al., 2016, 22.).

Consequences of a successful attack on hospitals can be wide-ranging:

Public Health and Safety Consequences: large number of deaths and injuries, in a biological attack on a hospital, the agent could be spread to the community through hospital staff or patient visitors. The attack would also impact local and regional emergency and public health services.

Economic Consequences: the costs of a terrorist attack on a hospital could be very high for victims and families, hospital owners, and insurance companies.

Social and Institutional Consequences: a large-scale attack on a hospital, that caused many casualties, could result in a fear of using hospital services among in the general public (URL6).

Cyber-attack: cause infliction of economic and operation damages, data theft, endangering patients' lives, unauthorized access to personal data etc.

Regulatory liability, plans

In Hungary, the Decree of the Ministry of Health No. 29/2000. (X. 30.) requires health care institutions to prepare disaster plans (URL15). The response and preparedness plan are inserted into the disaster plan. The fire safety plan of the institutions includes the evacuation plans prepared for specific departments or buildings. No explicit instructions are made for bomb threat and other terrorist acts. These are included in the action plan for the policing of crime and noticing detection of suspicious people. Workers are not trained what to do in a terrorist attack. They get just fire protection training and do not participate in simulation exercises. The western hospitals put on detailed plans for a public danger threat. A great emphasis is given to logistics, communication and information. Their purpose: review of Security/Risk Management Plans to assess the threat of a terrorist attack including a vulnerability assessment and possible preventative actions (URL6; URL18). American and British hospitals carry out simulation trainings. They gain experiences and measure the evacuation time of the hospital. According to experiences, there is bad communication towards the healthcare staff, so that they do not know when and what to do, who should propose evacuation, and as a result there were congestions in the staircases and delays in patients' evacuations. Domestic experts should take into account the experiences of these simulations and include them in their plans (URL17). A Canadian hospital in Ontario created and standardized an emergency color code system for Ontario hospitals and, on that basis, a protection plan that is used in almost every hospital in Canada. Each hospital ward has a code-based preventive or protective plan. (Code Orange Alert-Emergency Preparedness/ disaster Response Plan-St. Thomas Elgin General Hospital- Canada 2011.15.)

INCIDENT	NAME
Fire	Code Red
Cardiac Arrest	Code Blue
Internal Evacuation	Code Green
Missing Patient	Code Yellow
Bomb Threat or search	Code Black
Violent Person	Code White
Chemical Spill	Code Brown
Neo-Natal Arrest	Code Pink
External Disaster	Code Orange

Figure 3. Canadian Windsor Hospital's emergency code (by Hospital Windsor –Emergency Codes– Canada. 2010.(URL16)

According to experts, color coding is important because the use of the word color is less likely to cause panic than a specific word for threat or emergency, such as the sound of a fire on the speakers. Several hospitals in the United States use this code system. In connection with a terrorist attack the U.S. Department of Homeland Security (DHS) has developed the color-coded

Homeland Security Advisory System to communicate with public safety officials (see 4 Figure.).

Alert Level		Description
Red	SEVERE	Severe risk of terrorist attack
Orange	HIGH	High risk of terrorist attack
Yellow	ELEVATED	Significant risk of terrorist attack
Blue	GUARDED	General risk of terrorist attack
Green	LOW	Low risk of terrorist attack

Figure 4. DHS Advisory System Alert Level (by U.S.-Homeland Security Review, 2007.30.)

These measures are intended as a guide, they are not requirements under any regulation and legislation. U.S. hospitals make their security plans using indicators. Example: imminent attack indicators, surveillance indicators, transactional and behavioural indicators etc. They made protective measures, which aim are to protect the facility against threats and to mitigate the effects of an attack. Protective measures are designed to meet one or more of the following objectives:

Devalue: lower the value of a facility for a terrorist, that is, make the facility less interesting as a target.

Detect: spot the presence of adversaries and/or dangerous materials and provide responders with information needed to mount an effective response.

Deter: make the facility more difficult to attack successfully.

Defend: respond to an attack to defeat adversaries, protect the facility, and mitigate any effects of an attack (URL6).

Summary

In my article I presented and insisted on the fact that it would be necessary for all hospitals to have a preparedness plan for terrorist attacks, whose effectiveness is demonstrated by the simulation trainings. They should collaborate with area hospitals and hospital associations to address the threat of a terrorist attack and how to minimize the threat and respond to possible terrorist attack, cooperate with local, state and federal officials to improve communication regarding the threat of a terrorist attack and to increase the funding needed to prevent such an attack. The hospital is a special institute with immobile patients; therefore, its evacuation needs special plans. Hospitals in Hungary have not created adequate plans to address terrorism beyond mass casualty events and are therefore vulnerable to direct attacks by terrorists. Hungarian hospitals should study the plans of Western hospitals and learn, get ideas and useful information from them.

We could see in the essay, that in many countries hospitals have been targets of terrorist attacks (mostly in conflict zones). Terrorism is highest level of violence and all the institutions within the critical infrastructure have to be prepared for the potential risk. Hospitals are soft targets, where it is very easy to cause mass panic, and to influence public opinion, what is the main purpose of terrorists.

I find it useful to use the colour codes used by foreign hospitals, even though, according to some experts, this would increase administrative work and cause more confusion in the institutes. I think using a color code system can help to avoid mass panic, as we know that in the case of a terrorist attack, panic is a dangerous factor and terrorists benefit from it. That hospital management carries out a good work, which thinks about secure future and protects the values of patients and of the staff in the institute. This includes continuous trainings for employees, testing of theoretical knowledge, simulation trainings, and preparation of precise action plans and scenarios.

References

Besenyő, J. – Deák, G. (2010): *A biztonság* új *aspektusai: a kórházi személyzet bizonsága -A kórházi erőszakos cselekedetek megelőzése [New Aspects of Security: The hospital staff safety - The Prevention of Hospital Violence].* Székesfehérvár: MH ÖHP Tudományos Tanácsának Kiadványa

Besenyő, J. (2016): *Security preconditions: Understanding migratory routes.* Journal of Security and Sustainability Issues, 1, 5–26. DOI: 10.9770/jssi.2016.6.1(1)

Code Orange Alert-Emergency Preparedness/disaster Response Plan-St.Thomas Elgin General Hospital- Canada 2011. 15.(manuscript)

Finucane, J. D. (2017): *Unhealthy complacency: The vulnerability of US hospitals to direct terrorist attacks.* American Society for Healthcare Risk Management of the American Hospital Association, 9, 6. DOI: https://doi.org/10.1002/jhrm.21282

Deák, G. (2011)*: Are Hungarian hospitals able to manage terror acts, bomb threats?* Tradecraft review, Periodical of the Scientific Board of Military Security Office Special issue, 1, 129-133.

De Cauwer, H. (et.al.) (2016): *Hospitals: Soft Target for Terrorism?* Published online by Cambridge University Press, 94-100. DOI: https://doi.org/10.1017/S1049023X16001217

John, E. N. (1983): *A Guide to Hospital Security*. Gower Publishing C.L. Aldershot, 10-18.

Pascal, A. M. (1977)*: Hospital Security and Safety.* Aspen System Corporation, Rockville, Maryland, 3, 111.

Ráczkevy-Deák, G. (2013)*: Görbe tükör: a magyar kórházak katasztrófavédelmi helyzete napjainkban [Curved Mirror: The recent Disaster Protection Situation of Hungarian Hospitals].* Bolyai Szemle, 1, 177-180.

Russel, L. C. (2010): *Hospital and Healthcare Security*. *Fifthy Edition*. Boston: Butterworth-Heinemann, 10-15.
Tálas, P. (2006): *A terrorizmus anatómiája [The anatomy of terrorism]*. Budapest: Zrínyi Kiadó, 66.

Online Links in This Article

URL1: *Green Paper on a European Programme for Critical Infrastructure Protection*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN
URL2*: 2080/2008. (VI. 30.) Kormány határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról [Govern. Decree no. 2080/2008 on National Program of Critical Infrastructure Protection]*. http://www.njt.hu/cgi_bin/njt_doc.cgi?docid=120562.173569
URL3: *Terrorism 2002-2005*. http://www.fbi.gov/stats-services/publications/terrorism-2002-2005
URL4*: United Nations: Measures to eliminate international terrorism.* http://www.undemocracy.com/A-RES-49-60.pdf
URL5: John, E. (2016): *In the Crosshairs: Are Hospitals Targets for Terrorists Attacks?* https://www.usconcealedcarry.com/blog/crosshairs-hospitals-targets-terrorists-attacks/
URL6: *U.S. Department of Homeland Security: Hospitals. Potential Indicators of Terrorist Activity, Common Vulnerabilities, and Protective Measures.* https://www.calhospitalprepare.org/sites/main/files/file-attachments/cvpipm_report_hospitals_2.pdf
URL7: *Elfogták a bugyonnovszki csecsen támadás egy résztvevőjét [An accomplice of the Chechen attack in Budyonnovsk captured]*. http://index.hu/kulfold/bugy9042/
URL8: *A kórház igazgatóját is felelősségre vonják a Mozdoki tragédia miatt [Also the director of the hospital is called to account because of the tragedy in Mozdok]*. http://www.origo.hu/nagyvilag/20030802akorhaz.html
URL9: *The Sunday Times: 30 die in bomb attack on Iraq hospital.* http://www.timesonline.co.uk/tol/news/world/iraq/article596165.ece
URL10: *Bomba robbant egy pakisztáni kórházban [Bomb explosion in a hospital in Pakistan]*. http://hirek.myrss.hu/hir/243901/bomba-robbant-egy-pakisztani-korhazban.html
URL11: *Merénylet a kórház előtt [Attempt in front of the hospital]*. http://hirek.myrss.hu/hir/292889/merenylet-a-korhaz-elott
URL12: *Pak tribune: Terrorists kill five in Lahore hospital attack.* http://www.paktribune.com/news/index.shtml?228095
URL13: *A Cybersecurity Threat Model for a Combined Cyberattack against Hospitals and Terrorist Attack in Spain. http://www.fundacionasisa.org/documents/cybersecurity-threat-model.pdf*
URL14: *The cyber threat against the Danish healtcare sector.* https://fe-ddis.dk/cfcs/publikationer/Documents/2018_Threat_Assessment_Cyber_Threat_Danish_Healthcare.pdf
URL15: *29/2000. (X. 30.) EüM rendelet az egészségügyi intézmények katasztrófaterveinek tartalmi követelményeiről [Ministry of Healthcare decree 29/2000 (X.30.) on content require-*

ments of disaster protection plans in health institutions]. http://njt.hu/cgi_bin/njt_doc.cgi?docid=48681.251927
URL16: *Hospital Windsor Canada*. https://www.wrh.on.ca/
URL17: *Hancock, Charles-Johnson, W. Chris (2005): Thinking the unthinkable. Exposing the Vulnerabilities in the NHS Response to coordinated terrorism actions.* http://www.dcs.gla.ac.uk/~johnson/papers/NHS_terrorism.pdf
URL18: Rogers, C. M.: *The Rogers Law Firm Boston, MA: The Liability Risk of Hospitals as a Target of Terrorism.* http://www.ehcca.com/presentations/emsummit2/4_02.pdf
URL19: *Nearly Half of the Norway Population Exposed in HealthCare Data Breach.* https://thehackernews.com/2018/01/healthcare-data-breach.html
URL20: *UK hospital meltdown after ransomware worm uses NSA vuln to raid IT.* https://www.theregister.com/2017/05/12/nhs_hospital_shut_down_due_to_cyber_attack